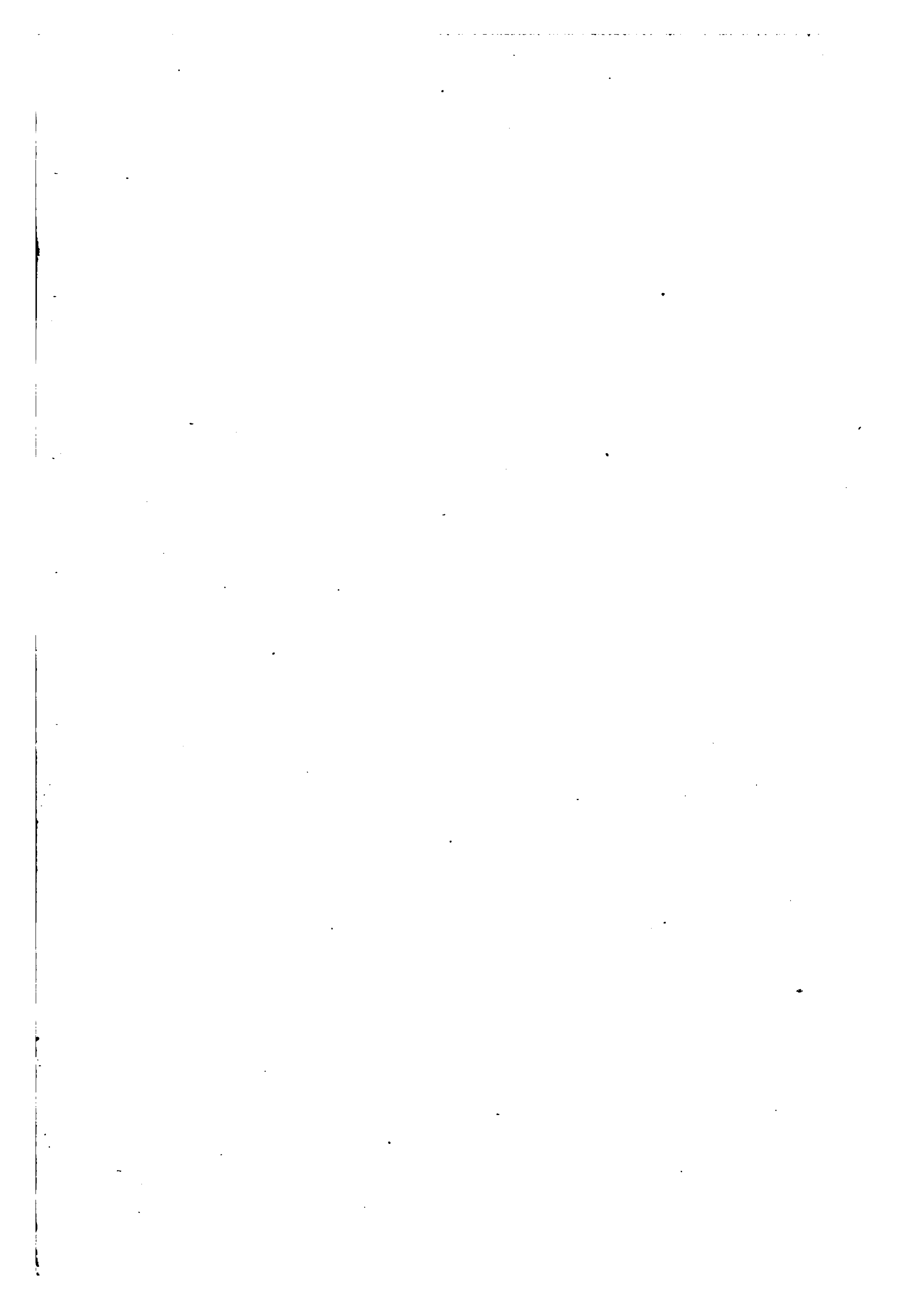

SIGILLVM ACADEMIAE HARVARDIANAE IN NOV·ANG
CHRISTO ET ECCLESIAE
VE RI TAS





Geschichte

der

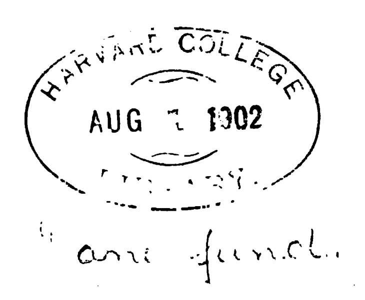
Gleichung $t^2 - Du^2 = 1$.

Von

Dr. H. Konen.

Mit 2 Figuren im Text.

Leipzig
Verlag von S. Hirzel
1901.


HARVARD COLLEGE
AUG 7 1902

Vorwort.

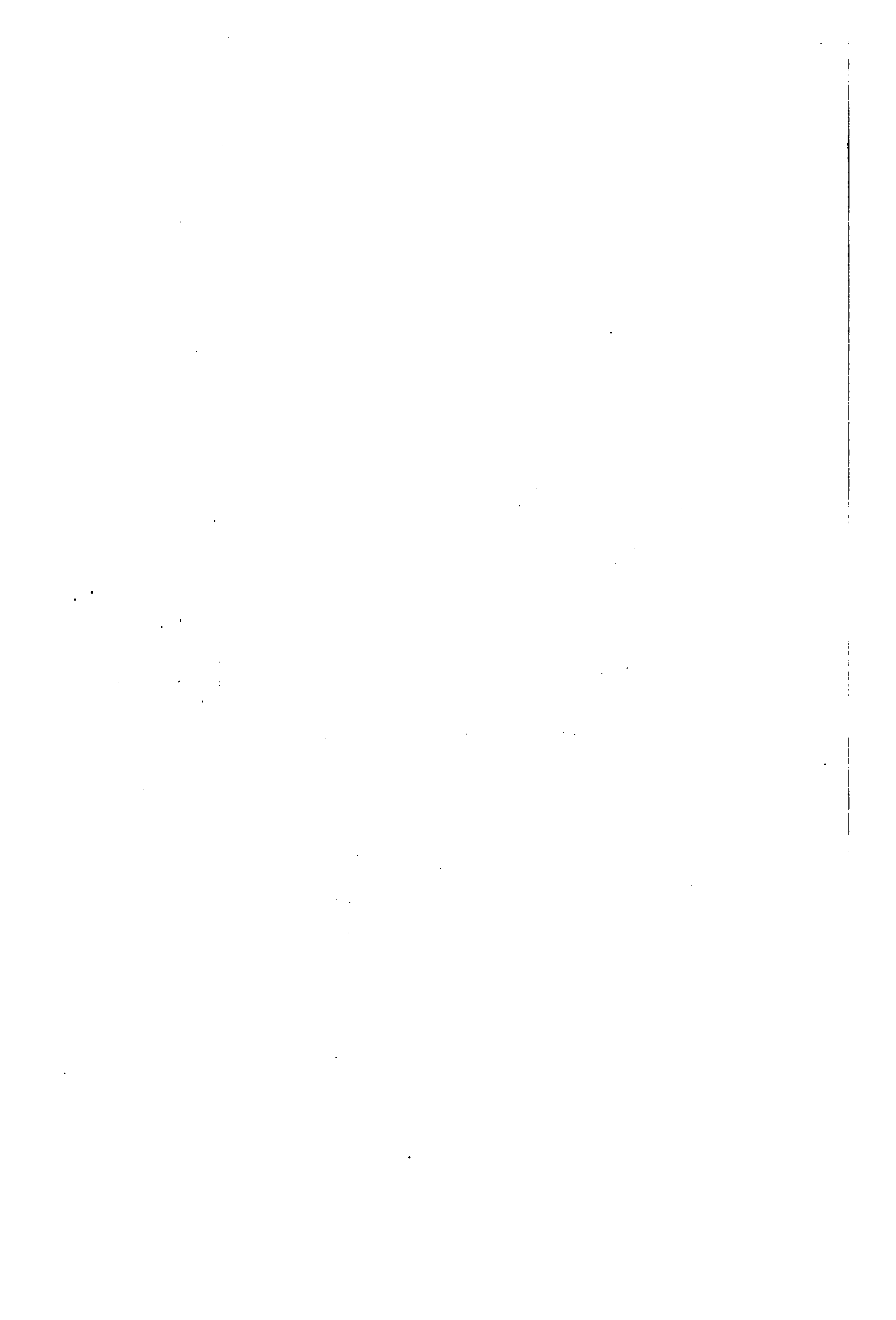
Die Bedeutung der ganzzahlig zu lösenden Gleichung $t^2 - Du^2 = 1$ in fast der gesamten Zahlenlehre rechtfertigt wohl den Versuch einer kleinen Geschichte eines Gegenstandes, der während 2000 Jahren die grössten Mathematiker aller Zeiten beschäftigt hat. Die Darstellung wendet sich in erster Linie an jüngere Mathematiker, schliesst vor Kronecker ab und benutzt nur die Mittel der elementaren Zahlenlehre. Das Bestreben des Verfassers ging dahin, das reichliche Material recht vollständig zu geben, den Leser, wo es möglich war, zum Originale selbst zurückzuführen und ihm als Vorbereitung zu dienen auf das Studium unserer grossen mathematisch-historischen Werke. Mit der Annäherung an die Jetztzeit war in Rücksicht auf unsere vortrefflichen Lehrbücher grössere Kürze geboten, doch erforderte der Zweck der Schrift eine wenn auch kurze Darstellung der geläufigen Methoden.

Es ist mir eine angenehme Pflicht, auch an dieser Stelle drei Herren meinen besonderen Dank auszusprechen, Herrn Geh. Prof. Dr. R. Lipschitz zu Bonn, der mich zu der Arbeit anregte, und den Herren Hofrat Prof. Dr. M. Cantor zu Heidelberg und G. Eneström in Stockholm, die mich mit Rat und That auf das liebenswürdigste unterstützten.

Bonn, im August 1901.

H. Konen.

Inhalt.



Die ganzzahlige Auflösung der Gleichung $t^2 - Du^2 = 1$ ist eines der ältesten Probleme, mit welchen sich die Arithmetik befasst hat. Schon die Griechen lösten es in speziellen Fällen und hatten es höchst wahrscheinlicher Weise auch im allgemeinen ins Auge gefasst.[1]) Die indischen Mathematiker beschäftigten sich viel mit ihm, und es gelang ihnen, eine Lösungsmethode zu finden, welche Hankel[2]) für „das Feinste" erklären zu dürfen glaubt, „was in der Zahlenlehre vor Lagrange geleistet worden ist".

Mittlerweile waren die arithmetischen Studien im Abendlande fast in Vergessenheit geraten. Erst als man nach dem Erwachen der klassischen Studien das Werk Diophants wieder kennen lernte, blühten sie neu auf, und unter den glänzenden Entdeckungen und tiefen Problemen, mit denen ein Fermat die junge Wissenschaft bereicherte, befand sich auch die Stellung und Lösung unserer Aufgabe.

Sie hat von da ab nicht aufgehört, die ersten Mathematiker zu beschäftigen. Die Namen Brancker, Euler, Lagrange, Gauss, Jacobi, Dirichlet, Kronecker bezeichnen den Gang dieser Entwicklung, die aufs engste verknüpft blieb mit den Fortschritten der Arithmetik überhaupt und eine ungeahnt ausgedehnte und tiefe Bedeutung der Theorie der Gleichung $t^2 - Du^2 = 1$ in fast der gesamten Zahlenlehre aufdeckte.

Es wird im folgenden unsere Aufgabe sein, die Stadien dieser Entwicklung von den ersten Anfängen an zu verfolgen. Die Lösungsmethoden der verschiedenen Perioden im Verein mit den mannigfachen Irrwegen, die man beschritt, werden uns dann einen Ausblick liefern auf die Entwicklung der Zahlenlehre selbst.

1) P. Tannery, Sur la mesure du cercle d'Archimède. Mém. de la soc. des sciences phys. et nat. de Bordeaux, IIième série Tome IV. p. 325. Bordeaux 1882.

2) Hankel, Zur Geschichte der Mathematik im Altertum und Mittelalter. 8°. Leipzig 1874. p. 200.

I. Teil: Bis zu Fermat.

§ 1. Die ganzzahlige Auflösung der Gleichung bei den Griechen.

Die ältesten Spuren unserer Gleichung verlieren sich in dem Dunkel, das über der Mathematik der Pythagoreer schwebt. Erst aus der Zeit Platos[1]) erhalten wir deutlichere Nachrichten, die sich in den Kommentaren zu den Werken des grossen Philosophen bis ins fünfte Jahrhundert n. Chr. hinziehen, um dann im Abendlande für 1000 Jahre auszusetzen. Und die wenigen Quellen selbst, die wir besitzen, fliessen nur spärlich.

Da sind zunächst die Andeutungen bei Plato in Kap. VIII der *Πολιτεία*[2]), der berüchtigten Stelle, wo von der hochzeitlichen oder geometrischen und der göttlichen oder vollendeten Zahl die Rede ist.[3]) Hierbei wird von Plato auch die *ῥητὴ διάμετρος πεμπάδος* und die *ἄρρητος διάμετρος* herangezogen.

Die Bedeutung dieser Bezeichnungen ist nun nach Cantor die folgende.

Bekanntlich behandelten die Griechen auch die Arithmetik in geometrischem Gewande, indem sie jede Zahl durch eine Strecke, ein Rechteck oder ein Parallepided, oder umgekehrt jedes der genannten geometrischen Gebilde durch eine Zahl darstellten.[4])

---

1) Man vergl. M. Cantor, Vorlesungen über die Geschichte der Mathematik Bd. I. 1. Aufl. Leipzig 1880 bei Teubner. 2. Aufl. Leipzig 1894. S. 210, 211. Im folgenden soll durch einen Index an der Band-Nummer die Auflage bezeichnet werden.

2) Platonis rei publicae libri decem ed. C. F. Hermann. VIII, 546. B. C. p. 236. Die Stelle lautet: „*ἀπὸ διαμέτρων ῥητῶν πεμπάδος, δεομένων ἑνὸς ἑκάστων, ἀρρήτων δὲ δυεῖν.*

3) Zu der Stelle, die eine ganze Literatur für sich hervorgerufen hat, Cantor, l. c., I_2, S. 210; ferner F. Hultsch, Die Pythagoreischen Reihen der Seiten und Diagonalen von Quadraten und ihre Umbildung zu einer Doppelreihe ganzer Zahlen. Bibl. Math. I. S. 8—12 (1900). — F. Hultsch in Procli Diad. in Platonis rem publicam commentarii, ed. G. Kroll, Vol. II, Leipzig 1901. S. 393—400.

4) F. Hultsch, Die Pythagoreischen Reihen etc. S. 9, Anm. 1. — Ders. bei Kroll. S. 395, Anm.

So ist nun bei Plato nach Cantor von der Länge der Diagonale des Quadrates über der Seite 5 die Rede, die rational ausfalle, wenn man den Radikand 50 um 1 verringere, bei Abzug von 2 jedoch irrational bleibe. Demnach war $\sqrt{2\cdot 5^2}$ die ἄρρητος διάμετρος, $\sqrt{2\cdot 5^2 - 1} = 7$ die ῥητὴ διάμετρος der Zahl 5.

Die letztgenannte Zahl stellt daher einen Näherungswert für $\sqrt{50}$ und $\frac{7}{5}$ somit eine Näherung für $\sqrt{2}$ dar.

Es liegt nahe, den gleichen Versuch, der bei der Zahl 5 zum Ziele führt, auch mit anderen „Seitenzahlen" zu machen, d. h. zuzusehen, wann $2a^2 - 1$ ein Quadrat sei. Dann leuchtet aber unmittelbar ein, dass die Identität $2a^2 - 1 = b^2$ oder $2a^2 + 1 = b^2$ keineswegs für alle ganzzahligen Werte von a zutrifft.

So werden wir auf natürliche Weise zu einem Spezialfall unserer Gleichung geführt, und es ergiebt sich zugleich der Zusammenhang mit der näherungsweisen Bestimmung der Quadratwurzeln, die seit dem ersten Studium der Irrationalitäten durch die Pythagoreer eine so bedeutende Rolle in der griechischen Mathematik spielen.[1]

Dass in der That der oben bezeichnete Weg eingeschlagen wurde und dass jener Platostelle somit wirklich diese tiefere und auf die Pythagoreer zurückweisende Beziehung beizulegen ist, geht aus den späteren Kommentaren hervor, die wir besitzen.

Hier ist zunächst eine Stelle bei Theon Smyrnäus[2] zu nennen, auf welche nach einer Bemerkung Günthers[3] zuerst Unger[4] aufmerksam gemacht hat.

---

1) Man vergl. die Ausführung bei Cantor (Bd. I_2, S. 211) über die Gründe, die dafür sprechen, dass Plato gewusst und in der Praxis benutzt hat, dass $\sqrt{2}$ angenähert gleich $\frac{7}{5}$.

2) Theon von Smyrna lebte um 130 n. Chr. Sein Werk: *Τῶν κατὰ μαθηματικὴν χρησίμων εἰς τὴν τοῦ Πλάτωνος ἀνάγνωσιν* ed. Hiller, Leipzig bei Teubner, oder éd. et traduit par S. Dupuis, Paris, Hachette, 1893. Kap. 31: *περὶ πλευρικῶν καὶ διαμέτρων ἀριθμῶν* (Hiller, S. 43, Dupuis, S. 71—75) verfolgt den ausgesprochenen Zweck, die zum Studium Platos notwendigen mathematischen Kenntnisse vorzutragen. Hierzu Cantor, Bd. I_2, S. 144 und 404—409.

3) Siegm. Günther, Die quadratischen Irrationalitäten der Alten und deren Entwicklungsmethoden. Abhandl. zur Gesch. der Math. IV. Zs. Math. u. Phys., Suppl. zur histor.-lit. Abt. (1882). S. 23.

4) Unger, Kurzer Abriss der Geschichte der Zahlenlehre von Pythagoras bis auf Diophant. Gymn.-Progr. Erfurt 1843. Ich konnte das Büchlein nicht erhalten. Doch erscheint dieser Schrift gegenüber Nesselmann als der ältere, dessen „Algebra der Griechen" 1842 erschien.

Ausgehend von zwei Einheiten, bildet Theon nach den Formeln

$$a_{n+1} = a_n + d_n; \qquad d_{n+1} = 2a_n + d_n$$
$$a_0 = 1; \qquad d_0 = 1$$

zwei Reihen von Zahlen a_{n+1} und d_{n+1} und giebt ohne Beweis die Regel $d_n^2 = 2a_n^2 + 1$.

Die Zahlen d_n heissen διάμετροι, die Zahlen a_n πλευραὶ aus schon erwähnten Gründen.[1])

Der Beweis, der bei Theon fehlt, lässt sich nach Günther[2]) etwa so ergänzen

$$\begin{aligned} d_n^2 - 2a_n^2 &= (2a_{n-1} + d_{n-1})^2 - 2(a_{n-1} + d_{n-1})^2 \\ &= -(d_{n-1}^2 - 2a_{n-1}^2)^2 = (-1)^2(d_{n-2}^2 - 2a_{n-2}^2) \text{ etc.} \\ &= (-1)^{n+1}. \end{aligned}$$

Da wir durch einen glücklichen Zufall über den Weg orientiert sind, den die Griechen wirklich einschlugen, so bietet es ein besonderes Interesse, die verschiedenen Versuche zu verfolgen, die vor jener Entdeckung gemacht wurden, um die Herkunft und Bedeutung der Ausführungen bei Theon zu erklären und sie zu ergänzen.

Nesselmann[3]) sah noch in der erwähnten Stelle ein gelegentliches Aperçu Theons, eine Art Spielerei. Theon habe gesehen, dass das gleichschenklige rechtwinklige Dreieck, resp. die Gleichung $y^2 = 2x^2$ nicht ganzzahlig lösbar sei und es nun mit der Abänderung $y^2 = 2x^2 + 1$ versucht. Er habe in der Annahme

$$\begin{aligned} b^2 - 2a^2 &= 1 \\ b + a &= a' \\ b + 2a &= b' \end{aligned}$$

gesetzt und

$$b_1^2 - 2a_1^2 = 2a^2 - b^2 = 1$$

erhalten, dann weiter aus

$$\begin{aligned} a_1 + b_1 &= a_2 \\ 2a_1 + b_1 &= b_2 \\ b_2^2 - 2a_2^2 &= 1, \end{aligned}$$

1) Die Theon jedoch nicht nennt.

2) S. Günther, Die quadratischen Irrationalitäten etc. Zs. Math. Phys. lit.-hist. Abt. Suppl. S. 23 u. f. (1882).

3) Nesselmann, Algebra der Griechen. Berlin 1842. S. 228 u. f.

also eine neue Lösung gefunden. So könne man fortfahren; nun sei aber

$$a = 1 \qquad b = 1$$

eine evidente Lösung; man habe also bekommen

$$\begin{array}{lll} a = 1 & b = 1 & 2a^2 - b^2 = 1 \\ a_1 = 2 & b_1 = 3 & 2a_1{}^2 - b_1{}^2 = -1 \\ a_2 = 5 & b_2 = 7 & 2a_2{}^2 - b_2{}^2 = 1 \text{ u. s. w.} \end{array}$$

Bei einer ungeraden Anzahl k werde nun

$$\Sigma\, 2a_k{}^2 = \Sigma b_k{}^2$$

und damit sei die Analogie mit den Diametral- und Seitenzahlen

$$y^2 = 2x^2$$

vollständig gewesen.

Hingegen legte schon Unger[1]) der Stelle bei Theon grössere Bedeutung bei. Seine Bemerkung blieb jedoch unbeachtet, bis Cantor[2]) den Zusammenhang der Lösung der Gleichung $d_n{}^2 = 2a_n{}^2 \pm 1$ mit den Näherungsbrüchen für $\sqrt{2}$ in den Vordergrund stellte, mit besonderer Rücksicht darauf, dass das Bildungsgesetz der Diametralzahlen mit dem der Näherungsbrüche für

$$1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 \,.}}}$$

übereinstimmt. Man müsse annehmen, dass die Griechen zwar nicht die Form, jedoch der Sache nach die Kettenbrüche gekannt haben. Zugleich wies Cantor auf die enge Beziehung zur Streitfrage über den Ursprung der Näherungswerte quadratischer Irrationalitäten bei Archimed und auf die Möglichkeit hin, dass jene Theorie der Diagonalzahlen von Plato herrühre. Tannery[3]) schliesst sich dem an und hält es für in

1) Unger, Kurzer Abriss der Geschichte der Zahlenlehre von Pythagoras bis auf Diophant. Gymn. Progr. Erfurt 1843.

2) Cantor, Bd. I. S. 369 u. f. 1880. Bd. I_2. S. 302, 408–409.

3) P, Tannery, L'éducation Platonicienne. Revue philosophique. tome XI. p. 291. — Mém. de la soc. des sc. physiques et nat. de Bordeaux. IIième sér. tome I. p. 45. — L'arithmétique des Grecs dans Pappus. Mém. de la soc. des sc. phys. et nat. de Bordeaux. IIième série. tome III. Paris und Bordeaux 1880. p. 368. — L'arithmétique des Grecs dans Héron d'Alexandrie. ibidem. IIième série. tome IV. 1882. p. 171.

hohem Masse wahrscheinlich, dass man mit dem Studium der Gleichung $t^2 - 2u^2 = 1$ schon zu Lebzeiten Platos begonnen habe, Theon also nicht Original sei, wenn er auch vielleicht erst die vollständige Lösung gefunden habe.

Auch Günther[1]) ist der gleichen Ansicht.

Eine geistreiche, nach Art der Griechen rein geometrisch gehaltene Ableitung des Bildungsgesetzes der Diametralzahlen gab dann P. Bergh.[2]) Wir lassen sie hier folgen wegen des interessanten Vergleichs mit der originalen griechischen Methode.

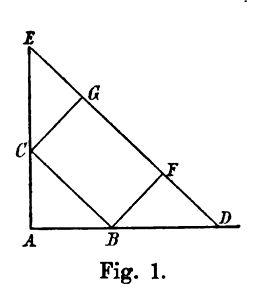


Fig. 1.

Nennen wir in dem gleichschenklig-rechtwinkligen Dreieck ABC die Länge AB a_{n-1}, die Länge BC $\mathfrak{d}_{n-1}$ und verlängern AB und AC um BD und CE gleich CB gleich $\mathfrak{d}_{n-1}$, so wird

$$AD = AE = a_{n-1} + \mathfrak{d}_{n-1} = a_n$$
$$DE = \mathfrak{d}_n.$$

Fällen wir ferner die Lote BF und CS, so sind die spitzen Winkel bei D, B, C und E sämtlich gleich 45^0, die Dreiecke DFB, BAC, CGE sind kongruent und man hat

$$DF = AB = a_{n-1},$$
$$\mathfrak{d}_{n-1} = GF = ED - 2FD = \mathfrak{d}_n - 2a_{n-1}, \text{ somit}$$
$$\mathfrak{d}_n = \mathfrak{d}_{n-1} + 2a_{n-1}$$
$$a_n = a_{n-1} + \mathfrak{d}_{n-1}.$$

„Natürlich ist die hier gezeigte Konstruktion falsch, insofern die Diagonale des Quadrates irrational ist; aber um immer nähere Werte zu erhalten, muss man geometrisch von der falschen Hypothese einer rationalen Diagonale ausgehen.“ [3])

So war die Frage nach Herkunft und Bedeutung der Diametral- und Seitenzahlen zum Stillstand gekommen, als 1900 von Kroll[4]) die

---

1) Siegm. Günther, Spezialfall der Pellschen Gleichung. Blätter für das bairische Real- und Gymnasialschulwesen. Band XVIII. S. 19 u. f. München 1884. — Günther, Die quadratischen Irrationalitäten etc. Leipzig 1882. S. 23. § 6.

2) P. Bergh, Seiten- und Diametralzahlen bei den Griechen. Zeitschr. Math. Phys. 31 (1886), historisch-literarische Abteilung. S. 135.

3) Entnommen aus einer brieflichen Mitteilung M. Cantors.

4) Proclii Diadochi in Platonis rem publicam commentarii ed. Guil. Kroll. Bd. I. Leipzig 1899, Teubner. Bd. II ib. 1901. Bd. II, S. 24—25, 27—29.

Abhandlungen von Proclus [1]) zu Platos Büchern vom Staate neu herausgegeben wurden. Die Lücke, die noch in der ersten Ausgabe von Schöll [2]) geblieben war, fand sich in dem benutzten Vatikanischen Manuskript ausgefüllt und neben vielem anderen waren auch Beiträge darin enthalten, die über unseren Gegenstand Licht verbreiteten und sogleich von Hultsch [3]) ausgenutzt wurden. Seiner Darstellung werden wir uns im folgenden anschliessen.

Proclus knüpft an die bereits erwähnte Stelle aus Platos Staat an und giebt uns bei Erläuterung der Begriffe *πλευρά* und *διάμετρος* (*ῥητή* und *ἄρρητος*) zugleich Auskunft über den Ursprung der Theorie, indem er diese ausdrücklich den Pythagoreern zuweist. Hultsch [4]) macht es wahrscheinlich, dass Proclus im Kapitel *κγ* aus Adrastos,[5]) im Kapitel *κζ* aus einer anderen Quelle, vermutlich aus der *μαθημάτων θεωρία* des Geminos [6]) schöpft. Immerhin berechtigt uns der ganze Charakter von Proclus' Ausführungen im Verein mit der Eigentümlichkeit der vorgetragenen Zahlenlehre, seinen ausdrücklichen Versicherungen, dass die in Rede stehenden Sätze den Pythagoreern angehörten, keinen Zweifel entgegenzusetzen." [7])

Hultsch [8]) zeigt ferner, dass auch die Ausführungen von Theon auf Adrastos fussen und wahrscheinlich aus dessen Kommentar zum Timaios geschöpft sind; dazu giebt Theon, wie Hultsch betont, selbst an, dass er nur *τὰ ὑπὸ τῶν Πυθαγορικῶν παραδοθέντα* paraphrasiere.

Auch der Umstand, dass bei Proclus die Proposition Buch II, Nr. 10 aus Euclids Elementen — also aus nachplatonischer Zeit — benutzt wird, spricht nicht gegen den Pythagoreischen Ursprung. Denn die meisten

1) Proclii comment. in remp. Platonis partes ineditae ed. R. Schoell. — Proclos, 410—485, Schulvorstand, Nachfolger Syrians (diadochus = Nachfolger) zu Athen, Philosoph und Mathematiker an der Universität. Seine Schriften sind eine Hauptquelle für die Geschichte der griechischen Mathematik. Vergl. Cantor, I_2. S. 463—466.

2) Fr. Hultsch, Die Pythagoreischen Reihen der Seiten und Diagonalen von Quadraten und ihre Umbildung zu einer Doppelreihe ganzer Zahlen. Bibliotheca mathematica. I. S. 8—12 (1900).

3) Fr. Hultsch in Prochli Diad. comm. ed Kroll. Bd. II. Excurs II. S. 393 bis 400 (1901).

4) Fr. Hultsch, Proclii in rem publ. comm. ed. Kroll. II. p. 393 (1901).

5) Adrastos, lebte im ersten Jahrhundert n. Chr., seine Schriften sind verloren gegangen.

6) Geminus lebte um 70 v. Chr. Sein verloren gegangenes mathematisches Werk wird von Proclus in seinem Kommentar zu Euclid vielfach benutzt.

7) Man vergl. Hultsch, l. c. S. 393—394.

8) Hultsch, ib. S. 393.

Sätze Euclids waren schon lange vor seiner Zeit bekannt; er ist in erster Linie Sammler und Bearbeiter,[1]) und gerade das zweite Buch ist mit dem grössten Teile seines Inhaltes Pythagoreischen Ursprungs, so dass wir vielmehr jene Proposition mit zurückdatieren müssen.[2]) So dürfte denn die Theorie der Diametral- und Seitenzahlen mit voller Sicherheit auf die Pythagoreer zurückzuführen sein und damit sind auch die ersten Studien über unsere Gleichung spätestens etwa in die Mitte des fünften Jahrhunderts v. Chr. zu verlegen, in Bestätigung der Vermutungen, die Cantor, Tannery und Günther schon vor dem Bekanntwerden des neuen Kommentars ausgesprochen hatten.[3])

Wenden wir uns nun zu dem mathematischen Inhalte der Ausführungen des Proclus.

Die Pythagoreer gingen aus von der Beobachtung, dass die Diagonale eines Quadrates von rationaler Seite irrational sei. Da somit keine Reihe von Zahlen möglich war, wo das Quadrat einer „Diagonalzahl" gerade gleich dem Doppelten des Quadrates einer „Seitenzahl" war, so bildeten sie eine Doppelreihe von Zahlen, wo der Unterschied zwischen dem Quadrat der Diagonalzahl und dem doppelten Quadrat der Seitenzahl ein Minimum war, nämlich ± 1. Zu je grösseren Seiten man dann aufstieg, um so kleiner wurde relativ der Unterschied.[4]) Da zugleich die Vorzeichen der Differenz wechseln, so ist die Summe der Quadrate zweier benachbarter Diagonalzahlen gleich der doppelten Summe der Quadrate der zugehörigen Seitenzahlen.[5]) Auch diese Folgerung erwähnt Proclus[6]) ebenso, wie früher Theon, indem er hinzufügt, dass die

1) Vergl. z. B. Cantor I_2. S. 259—260.

2) Fr. Hultsch, Proclii comm. ed. Kroll. II. p. 395—396 (1901). — Ders. Bibl. Math. I. p. 9—10 (1900).

3) Man vergl. S. 5, besonders Cantor I_2. S. 409.

4) Wie die Gleichung $t^2 - 2u^2 = \pm 1$ zeigt, liefert $\frac{t}{u}$ unmittelbar einen Näherungswert für $\sqrt{2}$. Denn, wie weiterhin (§ 4 u. f.) noch ausführlich erörtert werden wird, ist $\frac{t}{u}$ das Verhältnis von Zähler und Nenner der auf einander folgenden Näherungsbrüche der Kettenbruchentwicklung für

$$\sqrt{2} = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 \text{ etc.}}}}$$

(vergl. Cantor, I_2, S. 302 und 409).

5) Vergl. Nesselmann, Algebra der Griechen. Berlin 1842. S. 230.

6) Proclus, ed. Kroll. II. p. 25, 9—12. — Theon, ed. Hiller. S. 45, 2—8. — Hultsch bei Kroll. II. S. 398. — Man vergl. oben S. 5.

Summe aller Quadrate der Diagonalzahlen gleich der doppelten Summe der Quadrate aller Seitenzahlen sei.[1])

Kehren wir zu unserem Ausgangspunkt zurück, so handelte es sich zunächst darum, eine Reihe von „Seiten" zu finden, die der Beziehung $\partial_n{}^2 = 2\,a_n{}^2$ genügten (also irrational sind), aus denen sich dann die gewünschten, ganzzahligen Seiten ableiten liessen.

Hierzu dient ein Hilfssatz aus Euclids Elementen, Buch II. Der umständliche Wortlaut der bereits erwähnten 10ten Proposition lässt sich dahin zusammenfassen,[2]) dass, wenn eine Gerade AD in zwei Abschnitte $AB = BC$ und einen dritten beliebigen Abschnitt geteilt wird

$$\overbrace{A \quad B \quad C}^{}\!\!\underbrace{A \quad B}_{a}\underbrace{C \quad D}_{b} \qquad AD^2 + CD^2 = 2AB^2 + 2BD^2,$$

oder in algebraischer Form, die zugleich die Richtigkeit der Behauptung zeigt:

$$(a + b)^2 + b^2 = 2\left(\frac{a}{2}\right)^2 + 2\left(\frac{a}{2} + b\right)^2. \quad {}^{3})$$

Wie Proclus andeutet,[4]) wurde nun CD gleich der „Diagonale" gewählt; errichten wir die bezüglichen Quadrate (Fig. 2), so ist

$$AB = BC; \qquad CD = BE,$$

also

$$CD^2 = BE^2 = 2\,AB^2;$$

Fig. 2.

nach dem erwähnten Lehrsatz ist ferner

$$AD^2 + CD^2 = 2AB^2 + 2BD^2$$

1) Das stimmt genau natürlich nur für eine gerade Anzahl Glieder.

2) Hultsch, Bibliotheca Mathematica. I. p. 9 (1900). — Ders. in Proclus ed Kroll. II. p. 396 (1901). — Cantor, I_2, S. 249.

3) Cantor, I_2, S. 249. Der innere Zusammenhang leuchtet sofort aus der ersten der beiden Gleichungen ein, die das Gemeinsame zwischen den Diagonalen und Seiten einerseits und den Diagonalzahlen und Seitenzahlen andererseits enthält.

4) Proclus ed. Kroll. II. S. 27—28 giebt den geometrischen Beweis ohne Figur und nur für einen Fall. cf. Hultsch, Bibl. Math. I. S. 9—10, Anm. (1900).

und da

$$CD^2 = 2AB^2,$$

wird

$$AD^2 = 2BD^2.$$

Wie die Figur zeigt, ist aber auch

$$DF^2 = 2BD^2$$

und somit

$$DF = AD = 2AB + CD,$$

während

$$DB = AB + CD.$$

Gehen wir in gleicher Weise wie bisher vom Quadrate, über AB nunmehr von dem Quadrate über BD aus, so wird $DG = DB$, $GH = DF$ und wir erhalten, in derselben Weise wie eben, für die Diagonale HK des Quadrates über DH den Wert

$$HK = 2BD + FD,$$

während

$$HD = BD + FD.$$

So kann man offenbar beliebig weit fortfahren. Nennen wir die Seiten der Quadrate α_n, ihre Diagonalen ∂_n, so haben wir

$$\alpha_2 = \alpha_1 + \partial_1; \qquad \alpha_3 = \alpha_2 + \partial_2 \text{ etc.}$$
$$\partial_2 = 2\alpha_1 + \partial_1; \qquad \partial_3 = 2\alpha_2 + \partial_2 \text{ etc.}$$

Nunmehr ist alles bereit; setzen wir nämlich $\alpha_1 = 1$, so wird $\partial_1 = \sqrt{2}$; das war eine ἄρρητος διάμετρος, eine „unaussprechbare Zahl", wie oben $\sqrt{50}$ bei Plato; man ersetzte sie, von dem geometrisch richtigen Ansatze abweichend, durch die ῥητὴ διάμετρος, also 1. Verglich man nun aber die Quadrate der ῥητή und der ἄρρητος, so zeigte sich die Abweichung von der geometrischen Richtigkeit; denn während strenge

$$\partial_1{}^2 = 2\alpha_1{}^2$$

war, erhielt man jetzt

$$\partial_1{}^2 = 2\alpha_1{}^2 - 1.$$

Ferneres Einsetzen der gemachten Annahme ergab endlich die uns schon aus Theon bekannten Reihen der πλευραί, der Seitenzahlen und der διάμετροι oder Diagonalzahlen, nämlich

$$\alpha_1 = 1, \quad \alpha_2 = \alpha_1 + \partial_1 = 2, \quad \alpha_3 = \alpha_2 + \partial_2 = 5 \text{ etc.}$$
$$\partial_1 = 1, \quad \partial_2 = 2\alpha_1 + \partial_1 = 3, \quad \partial_3 = 2\alpha_2 + \partial_2 = 7 \text{ etc.}$$

Der allgemeine Beweis, dass nun in jedem Falle

$$\partial_n^2 - 2\alpha_n^2 = \pm 1$$

fehlt, jedoch ist der empirische Nachweis der Richtigkeit bei Proclus[1]) sowohl wie bei Theon[2]) bis zum 4ten Gliede zu finden, wie die folgende Tabelle zeigt:

α	∂	$2\alpha^2$	∂^2	Diff.
1	1	2	1	+ 1
2	3	$2 \times 2^2 = 8$	$3^2 = 9$	— 1
5	7	$2 \times 5^2 = 50$	$7^2 = 49$	+ 1
12	17	$2 \times 12^2 = 288$	$17^2 = 289$	— 1

Zum Schlusse fügt Proclus hinzu „καὶ ἀεὶ οὕτως“, behauptet also, dass sich die Reihe beliebig weit mit wechselnden Vorzeichen der Differenzen fortsetzen lasse.

Dass die Sache ihre Richtigkeit hat, haben wir bereits früher gesehen.[3])

Vergleichen wir den griechischen Gedankengang mit der oben gegebenen Ableitung Berghs, so zeigt sich, dass die letztere im Wesentlichen mit dem Original übereinstimmt, wenn man von der geringen Differenz in der Zeichnung der Figur absieht.

Nehmen wir die gleichfalls oben[4]) angeführte Bemerkung Cantors hinzu, so haben wir ein interessantes Beispiel für eine mathematische Rekonstruktion in antikem Geiste, wie man nicht gar zu viele findet.

Fassen wir nochmals das zusammen, was die Pythagoreer und mit ihnen Plato und seine Kommentatoren in betreff unserer Gleichung bestimmt wussten, so können wir die Resultate mit Hultsch[5]) in folgenden 3 Sätzen aussprechen:

1. Es giebt eine unendliche Reihe von Quadratzahlen (Diagonalzahlen zum Quadrat), deren Glieder sich von den doppelten Quadraten einer anderen Zahlenreihe (Seitenzahlen) nur um 1 unterscheiden.

---

1) Proclus ed. Kroll. Bd. II. p. 28, 10—29, 4.

2) Theon ed. Hiller. p. 43. Dazu Hultsch an den schon oft citierten Stellen.

3) Vergl. S. 4.

4) S. 6.

5) Hultsch, Proclus in rem. publ. ed. Kroll. II. p. 399.

2. Die Summe zweier benachbarter Quadrate der einen Reihe ist gleich der doppelten Summe der entsprechenden Quadrate der anderen.

3. Bildet man die Reihe der Verhältnisse jeder Diagonalzahl zu ihrer Seitenzahl, so erhält man immer genauere Näherungswerte für $\sqrt{2}$.

Es erübrigt uns nur noch einige andere Stellen zu nennen, die demselben Gedankenkreise angehören, ohne jedoch wichtige Beiträge zu liefern.

Sie finden sich bei Proclus[1]) selbst, bei Theon[2]) und bei dem Neuplatoniker Jamblichus.[3])

Wir wollen hier nur die Bemerkung Theons hervorheben, in der er sagt, jedes Quadrat sei von der Form $3x$, $3x+1$, $4x$ oder $4x+1$. Nach Tannery[4]) müsste man hieraus schliessen, dass die Griechen wussten, dass die Gleichung $t^2 - Du^2 = -1$ nicht immer ganzzahlig lösbar sei.

Damit ist im Grunde alles erschöpft, was wir Sicheres über die Beschäftigung der Griechen mit der Theorie unserer Gleichung aussagen können.

Alle sonstigen Nachrichten sind dunkel, widerspruchsvoll und ihre Auslegung strittig.

Die nächste Spur führt uns in die Zeit des grössten Mathematikers des Altertums, in die Zeit Archimeds.

Es ist das „problema bovinum", auf das wir uns beziehen.[5])

Die in 22 Distichen[6]) abgefasste „*Πρόβλημα ὅπερ Ἀρχιμήδης ἐν ἐπιγράμμασιν εὑρὼν τοῖς ἐν Ἀλεξανδρείᾳ περὶ ταῦτα πραγματευομένοις ζητεῖν ἐπέστειλεν ἐν τῇ πρὸς Ἐρατοσθένην τὸν Κυρηναῖον ἐπιστολῇ*"

---

1) Proclus, *Ὑπόμνημα εἰς Εὐκλείδην*. IV. p. 111. — Ders. in I. Eucl. elem. libr. ed. Friedlein. p. 427, 18—24. — Hierzu ferner: Cantor. II_2. p. 464. — Nesselmann, Algebra der Griechen. Berlin 1842. S. 230, 129. — Günther, Die quadr. Irrationalitäten etc. § 7. An beiden Stellen die Übersetzung.

2) Theon ed. Hiller. p. 35, 17.

3) Jamblichus, lebte Anfangs des 4. Jahrh. n. Chr.; gründete zu Chalcis in Cölesyrien eine Schule von Philosophen (Cantor, I_2, S. 429—431). Es ist hier Bezug genommen auf das vierte Buch der Sammlung der Pythagoreischen Lehren, der *συναγωγὴ τῶν πυθαγορικῶν δογμάτων* (man vergl. das oben über den Pythagoreischen Ursprung der Seitenzahlen etc. Ausgeführte). — Jamblichus Chalcidensis in Nicomachi Geraseni arithmeticam introductionem ed. Pistelli. p. 91, 3—93, 6. Dazu Nesselmann, Algebra der Griechen. Berlin 1842. S. 129 u. 230. — Günther, Die quadratischen Irrationalitäten etc. Leipzig 1882 etc. § 7.

4) Tannery, P., Sur la mesure du cercle d'Archimède Mém. de la soc. des sc. physiques et naturelles de Bordeaux. série II. Tome IV. 1882. Bordeaux et Paris. § IV.

5) Man vergl. zum Folgenden: Cantor. II_2. S. 297.

6) Nach Krummbiegel, der es zuerst bemerkte.

betitelte Aufgabe wurde 1773 aus einem Wolfenbütteler Kodex von Lessing veröffentlicht.[1])

Er sowie die beiden Struve[2]) verwarfen die im Titel behauptete Abstammung von Archimed, während Hermann[3]) zum entgegengesetzten Schlusse kam. Der letztere erzählt auch, nach einer mündlichen Mitteilung Mollweides habe Gauss sich mit dem Problem befasst und es vollständig gelöst, ohne jedoch darüber etwas veröffentlicht zu haben.

Nesselmann[4]) schliesst sich ohne Kenntnis der Hermannschen Schrift energisch der Meinung der beiden Struve an und meint, ebenso wie Klügel[5]) und Vincent,[6]) dass die Aufgabe nicht von den Alten herrühre. Schon wegen der ungeheuren Zahlen, auf welche sie führten, könnten die letzten Bedingungen des Problems nur von einem gedankenlosen Manne, nicht von dem grössten Mathematiker des Altertums herrühren.

Dieser Ansicht treten jedoch Heiberg[7]) und Tannery,[8]) ebenso wie früher Hermann entgegen, und auch die grosse kritische Arbeit von Krummbiegel und Amthor,[9]) in welcher nach dem Urteil so kompetenter Beurteiler wie Tannery[10]) und Günther[11]) die Frage ihren Abschluss gefunden hat, gelangt zum gleichen Resultate und weist die

1) Zur Geschichte der Literatur; aus den Schätzen der herzogl. Bibliothek zu Wolfenbüttel. 2. Beitrag von Gotth. Ephr. Lessing. Braunschweig 1773.

2) Altes griechisches Epigramm mathematischen Inhaltes, von Lessing erst einmal zum Druck befördert, jetzt neu abgedruckt und mathematisch und kritisch behandelt von Dr. J. Struve, Direktor des königl. Gymn. zu Altona und Dr. L. Struve, Direktor des städt. Gymn. zu Königsberg (Vater und Sohn). Altona 1821.

3) Gottfried Hermann, Universitätsprogramm. Leipzig 1828. Opuscula. Vol. IV. p. 228 u. f.

4) Nesselmann, Algebra der Griechen. Berlin 1842. p. 488 (mit Übersetzung).

5) Klügel, Mathematisches Wörterbuch. Teil I. p. 184.

6) Vincent, Nouv. ann. de mathemat. p. Terquem et Gerono vol. XV. Paris 1856. — Anhang: Bulletin de bibliographie etc. I, 39 fl.

7) Heiberg, Quaestiones Archimedeae. Dissert. Hauniae 1879. p. 25—27.

8) P. Tannery, L'arithmétique des Grecs dans Pappus. Mém. de la soc. des sc. physiques et nat. de Bordeaux. II. série. Tome III. Paris und Bordeaux 1880. p. 370.

9) Krummbiegel und Amthor, Das Problema bovinum des Archimedes. Zeitschrift für Math. herausg. von Schlömilch. Bd. XXV. 1880. Hist.-lit. Abteilung p. 121 u. p. 153. Abhandl. zur Geschichte der Math. III.

10) Tannery, P., Sur le problème des bœufs d'Archimède. Paris 1881. Bull. des sc. math. et astron. II. série. T. V. p. 25.

11) Günther, Die quadr. Irrationalitäten etc. Leipzig 1882. p. 92.

Lessingsche Aufgabe, wenn nicht der Form, so doch der Sache nach, Archimed selbst zu.

Damit gewinnt aber die Aufgabe von den Rindern des Heliôs ein besonderes Interesse für die Geschichte unseres Problems. Denn nach der Lösung der durch die ersten Bedingungen gegebenen, schon vom Scholiasten erledigten Gleichungen, führt die vorletzte Bedingung auf die ganzzahlig zu lösende Gleichung

$$t^2 - 47\,29\,494\,u^2 = 1,$$

während der letzte Vers noch fordert, dass u durch 4657 teilbar sei.

Amthor hat sich der Mühe der Berechnung unterzogen, $\sqrt{47\,29\,494}$ in einem Kettenbruch von 91gliedriger Periode entwickelt und so die kleinsten Auflösungen

$$T = 109\,331\,198\,673\,282\,973\,497\,986\,623\,282\,143\,354\,390\,108\,8049$$
$$U = 505\,494\,852\,343\,150\,330\,744\,778\,197\,355\,404\,089\,863\,40$$

gefunden. Mit Hilfe einer Reihe neuer Bemerkungen über die Teilbarkeit der Lösungen t_k und u_k durch gegebene Zahlen, kalkuliert Amthor ferner den kleinsten Wert von u_k, welcher der letzten Bedingung der Aufgabe genügen würde und findet, dass diese Zahl mit 206 546 Ziffern geschrieben werden müsse.[1])

Trotzdem Tannery[2]) auf Grund ausgedehnter, auch an diesem Problem gewonnener Erfahrungen im Rechnen mit griechischen Zahlzeichen und gestützt auf seine einzige Kenntnis der griechischen Arithmetik es für möglich hält, dass Archimed die Aufgabe, wenn auch vielleicht nicht in direkter Rechnung, löste, wird man, glaube ich, doch eher geneigt sein, Günther[3]) zuzustimmen, welcher meint, die Berechnung übersteige auf jeden Fall die Kräfte des Altertums.

Aus allem geht indes wohl hervor, dass Archimedes sich mit der Aufgabe der ganzzahligen Lösung der Gleichung $t^2 - Du^2 = 1$ auch im allgemeinen beschäftigt hat und sich zum mindesten der Schwierigkeit des Falles bewusst war, welchen er den Alexandrischen Mathematikern zur Lösung vorlegte; wenn es auch rätselhaft bleibt, wie er dazu gelangte, dies ohne Berechnung zu wissen.

---

1) Man wird, wie auch Amthor mit Recht bemerkt, bei solchen Zahlen unwillkürlich an die Sandrechnung des Archimedes erinnert. Vergl. auch d. f. b. Tannery.

2) P. Tannery, Sur le problème des bœufs etc. — Ders., L'arithmétique des Grecs etc. p. 370.

3) Günther, quadr. Irrat. etc. p. 92.

Wir haben bereits wiederholt auf den Zusammenhang zwischen der näherungsweisen Bestimmung von $\sqrt{2}$ und den Seiten und Diametralzahlen hingewiesen.[1]) Es ist nun bemerkenswert, dass man auch auf indirektem Wege, also von den thatsächlich überlieferten antiken Näherungswerten ausgehend, zu den gleichen Schlüssen über die Bekanntschaft der Alten mit der Gleichung $t^2 - Du^2 = 1$ gelangt. Denn es ist uns keine genauere Nachricht darüber erhalten, wie die Alten, zumal Archimed, zu jenen Werten für $\sqrt{3}$ etc. gekommen sind. Man ist also darauf angewiesen, in antikem Geiste gehaltene Berechnungsmethoden aufzusuchen und die von ihnen gegebenen Werte mit den überlieferten Näherungswerten zu vergleichen. Es ist nun bedeutsam, dass von allen Konstruktionen gerade diejenigen sich am besten bewähren, welche die Kenntnis und Benutzung der Auflösungen der Gleichungen $t^2 - Du^2 = 1$, $t^2 - Du^2 = 2$ voraussetzen.[2])

Wir dürfen wohl mit Cantor sagen, dass „sämtliche Versuche in einem Punkte zusammentreffen, nämlich in dem Bestreben, ein mehr oder weniger bewusstes Zusammentreffen der Methode des Archimedes mit dem modernen Kettenbruchverfahren nachzuweisen“. Am ausgesprochensten ist dies unter den älteren Versuchen bei Tannery der Fall, dessen Lösung Günther den Vorzug gab. Noch bestimmter stellt sich Hultsch auf diesen Standpunkt, indem er, gerade auf der Basis der Diagonal- und Seitenzahlen aufbauend und analytisch vorgehend, zu den Archimedischen Zahlenwerten zu gelangen sucht, ohne dass Hilfsmittel angewendet würden, die der Arithmetik der Alten fremd gewesen sein dürften.

Wir müssen uns jedoch versagen, hier genauer auf diese interessante Streitfrage einzugehen, und so erübrigt uns nur noch, von den griechischen

---

1) S. 3, 5.

2) Man vergl. hierzu Cantor I_2 S. 301—303, S. 210—211, S. 207—209, woselbst die Literatur; Zusammenstellung und ausführliche Kritik bis 1882 findet man bei Günther, Die quadr. Irrationalitäten etc. Zeitschrift für Math. Leipzig 1882. Supplement. § 14. Dazu ferner S. Günther, Antike Näherungsmethoden im Lichte moderner Mathematik. Abh. köngl. böhm. Ges. Wiss. (6). Bd. 9. Prag 1878. Heiberg, Quaestiones Archimedeae. Diss. Hauniae 1879. p. 60—66. Hunrath, Die Berechnung irrationaler Quadratwurzeln vor der Herrschaft der Dezimalbrüche. Kiel (1884). Tannery, Sur la mesure du cercle d'Archimède etc. Mém d. l. soc. d. sc. ph. et n. de Bordeaux 1882. II. sér. Tome IV. p. 303. Fr. Hultsch, Die Näherungswerte irrationaler Quadratwurzeln bei Archimedes. Nachr. v. d. Königl. Ges. d. Wiss. u d. G.-A-Univ. zu Göttingen 1893. S. 367—428. Daselbst weitere Literatur. Fr. Hultsch, Zur Kreismessung des Archimedes. Zeitschr. Math. Phys. 39. (1894) historisch-literarische Abt. S. 121—137, 161—172.

Mathematikern Diophant zu nennen, in dessen Arithmetik man wohl zu allererst nach einer Behandlung der Gleichung $t^2 - Du^2 = 1$ suchen möchte, wäre es auch nur für rationale t und u. Allein obwohl es häufig[1]) nur eines Schrittes bedürfte, um die rationale Auflösung der allgemeinen Gleichung zweiten Grades mit zwei Unbekannten auf eine Gleichung von der Form $t^2 - Du^2 = C$ zu reduzieren, wird dieser Schritt nicht gethan. Trotzdem soll Diophant mit unserem Problem nicht unbekannt gewesen sein. Ich lasse Tannery[2]) reden.

„A la verité, nous ne retrouvons pas ces problèmes dans Diophante, mais ils étaient sans doute traités dans les sept livres de son ouvrage, qui ne nous sont pas parvenus".

Das ist allerdings nur eine Vermutung, doch wird man ihr, meine ich, wohl beistimmen, wenn man sieht, wie nahe Diophant oft daran ist, unsere Gleichung zu behandeln; denn es hält trotz aller Systemlosigkeit Diophants schwer zu glauben, dass er den einen Schritt nicht gethan habe.

Dazu hat Tannery noch in höchst geistvoller Weise[3]) nur aus Schlüssen und Formeln, die sich wirklich bei Diophant vorfinden, eine Lösung der Gleichung $t^2 - Du^2 = 1$ zusammengestellt, die allerdings ebensowenig wie andere Ausrechnungen Diophants allgemein und vollständig ist, auch ohne Versuche nicht auskommt, aber wohl deutlich genug dafür spricht, dass, wenn wirklich Diophant niemals die Gleichung $t^2 - Du^2 = 1$ behandelte, dies nur einem bei einem solchen Manne kaum begreiflichen Zufall zuzuschreiben ist.

---

1) Man vergl. die Zusammenstellung bei Nesselmann, Algebra der Griechen. Berlin 1842. S. 331, 344. Doch geht Nesselmann mit seiner Systematik unzweifelhaft über das Original hinaus. Hierzu besonders: Hankel, Zur Geschichte der Mathematik im Altertum. Leipzig 1874. S. 164f. — Cantor. I_1. S. 398. I_2. S. 448.

2) P. Tannery, L'arithmétique des Grecs dans Pappus. Mém. soc. des sc. phys. de nat. de Bordeaux (2) t. 3. Paris et Bordeaux 1880. p. 370f.

3) Tannery, Sur la mesure du cercle d'Archimède. Mém. d. l. soc. d. sc. phys. et nat. de Bordeaux. Bordeaux 1882. II. sér. tome IV. p. 313. Dazu auch S. Günther, quadratische Irrationalitäten etc. Abhandl. zur Gesch. der Math. 4. Zs. Math. Phys. Suppl. hist.-lit. Abt. (1882). § 14 endlich P. Tannery, Études sur Diophante. Bibl. Math. 1887. p. 84—85. Hier verfolgt Tannery den Gedanken noch weiter. Er führt alle Eliminations-„Kunststücke" Diophants auf eine Grundmethode zurück und zeigt, wie sich in der That mit Hilfe derselben eine Auflösung der unbestimmten Gleichung 2. Grades mit zwei Unbekannten ergiebt und zwar ist es dieselbe, die man — in den betreffenden speziellen Fällen — wirklich bei Diophant findet. Das Verfahren umfasst aber auch unsere Gleichung.

Nach dem Besprochenen dürfte der Entwicklungsgang des Problems bei den Griechen etwa folgender gewesen sein.

Angeregt durch ägyptische,[1]) vielleicht babylonische Einflüsse brachten die Pythagoreer zum Studium der Mathematik die Neigung mit, Zahlengrössen und ihre Verknüpfungen geometrisch zu versinnlichen. So gelangten sie zum Begriff der Irrationalzahl oder vielmehr des Irrationalen, da den Pythagoreern die Irrationalzahl eine ἄρρητος, d. h. keine Zahl war.[2]) Von der Diagonale des Quadrates ausgehend, erfanden sie dann auf dem oben bei Proclus ausführlich beschriebenen Wege die Diametral- und Seitenzahlen, deren Verknüpfung eben durch einen Spezialfall unserer Gleichung gegeben war. So verlieren sich die ältesten Spuren eines Hauptgegenstandes der Zahlentheorie vielleicht im babylonischen und ägyptischen Altertum; mystisch-philosophische Spekulationen und die Verknüpfung der Arithmetik mit der Geometrie waren es, die zuerst die Gleichung $t^2 - Du^2 = 1$ in den Kreis wissenschaftlicher Forschung zogen.

Zu Platos Zeiten waren die Kenntnisse der Pythagoreer bereits allgemein verbreitet, so dass er in seinen Schriften sich ohne weiteres darauf berufen konnte.

In den Kommentaren zu Platos Werken lebten diese Kenntnisse dann fort, die Theorie der Seiten und Diametralzahlen wurde reproduziert. Vielleicht wegen ihrer Einfachheit, vielleicht wegen der Voraussetzungen Platos finden wir nur sie, vielleicht war sie auch der einzige Fall, den man kannte.

Wie sich nach Plato die Kenntnis der Gleichung $t^2 - Du^2 = 1$ weiter entwickelte, dafür fehlen alle Anhaltspunkte. Sicher ist jedoch dass von Archimedes und seit Archimedes das Problem in seiner Allgemeinheit gestellt wurde. Auch wurde es vielleicht rechnerisch gelöst. Es ist aber wohl zwischen der zur vollständigen Lösung erforderlichen Theorie und der praktischen halb experimentellen Berechnung zu unterscheiden. „Aucun des anciens n'a certainement possédé la première; une telle découverte eût été célèbre et elle ne se serait pas perdue sans laisser aucune trace.“[3])

Die Schwierigkeiten, welche sich der Begründung einer Theorie der

---

1) Cantor I_2. p. 138 u. f. p. 73.

2) Cantor I_2. p. 175.

3) P. Tannery, Sur la mesure du cercle d'Archimède. Mém. soc. d. sc. phys. et nat. de Bordeaux (1882). IIième sér. T. 4. p. 325.

Lösung entgegenstellten, und welche erst von Lagrange wirklich besiegt wurden, mögen es auch verschulden, dass uns so spärliche Nachrichten über die antiken Methoden überliefert sind.

§ 2. Die ganzzahlige Auflösung der Gleichung $t^2 - Du^2 = 1$ bei den Indern.

Schon Colebrooke,[1]) der Verfasser der Übersetzung indischer Mathematiker,[2]) soviel ich sehe, der einzigen Quelle für fast alle,[3]) die sich bisher mit indischer Arithmetik befasst haben, giebt in der Einleitung zu dem genannten Werke[4]) eine Übersicht über die Geschichte der Fermatschen Gleichung und weist der indischen, sogenannten cyklischen Methode zu ihrer Lösung einen hervorragenden Platz an; erst Euler und Lagrange hätten wiedergefunden, was die Inder schon gekannt. Buchner[5]) veranstaltete einen lateinischen Auszug aus Colebrooke, indem er sich die Aufgabe stellte, die schwer verständlichen indischen Regeln übersichtlich geordnet darzulegen, doch fehlt gerade das Wesentlichste der cyklischen Methode. In der kleinen Geschichte der Mathematik von Arneth[6]) ist die indische Arithmetik unverhältnismässig ausführlich dargestellt. Das Material ist aus Colebrooke geschöpft, doch rührt die Anordnung und Beziehung der Regeln von Arneth her. Ganz besonders gründlich und mit einer Art Begeisterung behandelt Hankel den Gegenstand.[7]) Seiner Darstellung will ich mich im folgenden anschliessen.

Cantor[8]) und Tannery[9]) endlich nehmen in Bezug auf Anord-

1) Algebra with arithmetic and mensuration from the Sanscrit of Bramegupta and Bhaskara translated by H. Colebrooke, London 1817.

2) Verzeichnis derselben bei Cantor. Geschichte I_1. S. 533 und I_2. S. 558. — Matthiessen, Grundzüge der antiken und modernen Algebra der literalen Gleichungen. Leipzig 1896. p. 967. — Der Sanskrittext zu Bhaskara (1141—1225) und Brahmegupta (gegen 598) herausgegeben von Kern. Leiden 1874.

3) Ausnahmen z. B. Rodet, Leçons de calcul d'Aryabhata. Journal Asiatique 1879. p. 15 u. p. 43. Es wird jedoch nur die Cuttaca behandelt, da sich die cyklische Methode bei Aryabhata (gegen 476 n. Chr.) nicht findet.

4) Colebrooke, l. c. Dissertation S. XVIII.

5) Buchner, De Algebra Indorum, Programm. Elbing 1821. p. 25 u. f.

6) A. Arneth, Die Geschichte der reinen Mathematik in ihren Beziehungen zur Geschichte der Entwicklung des menschlichen Geistes. Abgedruckt aus der „neuen Encyklopädie für Wissenschaften und Künste". Stuttgart 1852. S. 149 u. f.

7) Hankel, Zur Geschichte der Mathematik im Altertum und Mittelalter. Leipzig 1874. S. 180, 196, 198, 200 u. f.

8) Cantor, Vorl. über Geschichte der Mathematik. Bd. I_1. S. 533. I_2. S. 592.

9) P. Tannery, Sur la mesure du cercle d'Archimède. Mém. de la soc. d.

nung und Beurteilung einen etwas von **Hankel** abweichenden Standpunkt ein.

Das „cyklische" Verfahren zur ganzzahligen Auflösung der Gleichung $t^2 - Du^2 = 1$ findet sich dargestellt bei **Bhaskara** und **Brahmegupta.**[1]) Indem ich die Interpretation der indischen Regeln nach **Hankel** gebe, füge ich zugleich links die Stellen aus **Bhaskara** in der **Colebrookeschen** Übersetzung bei, auf welche man sich meiner Meinung nach zur Rechtfertigung der einzelnen Schritte berufen kann.

Vi'ja-Gan'ita. Chap. III. (Bhaskara.) Affected square. Section I (Colebrooke. p. 170).

§ 75. Vorbemerkungen. In der Gleichung $t^2 - Du^2 = 1$ darf D kein Quadrat sein. Es wird als positiv vorausgesetzt u die kleine, t die grosse Wurzel genannt.

§ 76. Having set down the „least" and „greatest" roots and the additive and having placed under them the same or others in the same order, many roots are to be deduced from them by composition. Werefore their composition is propoundet.

§ 77. The „greatest" and „least" roots are to be reciprocally multiplied cross wise; and the sum of the products to be taken for a least root. The product of the two „least" roots being multiplied by the given coefficient and the product of the greatest roots being added thereto, the sum is the corresponding grea-

Hilfsbemerkungen. Hat man p und q, p_1 und q_1 so gefunden, dass

$$Dq^2 + s = p^2,$$
$$Dq_1^2 + s_1 = p_1^2,$$

so erfüllen $u = pq_1 \pm qp_1$ und $t = pp_1 \pm qq_1 D$ die Gleichung $Du^2 + ss_1 = t^2$.

---

sciences phys. et nat. de Bordeaux. IIième série. Tome IV. Paris 1882. p. 313 u. f. Nr. III des Aufsatzes.

1) Daten nach **Bhau Dâji**: Brahmegupta gegen 593. Bhaskara gegen 1141 bis 1225. Dass Aryabhata (gegen 476 n. Chr.) nichts hat, rührt nach **Hankel** vielleicht daher, dass seine Schrift vorwiegend astronomischer Natur ist.

test root; and the product of the additives will be the (new) additive.

§ 78. Die gleiche Regel für das minus-Zeichen in $u = pq_1 \pm qp_1$, $t = pp_1 \pm qq_1 D$.

Zu § 77 giebt der Glossator Crisńa-Bhaťťa einen Beweis, welcher nach Colebrooke abgekürzt und in moderner Bezeichnung so lautet. Aus

$$Dq^2 + s = p^2,$$
$$Dq_1{}^2 + s_1 = p_1{}^2$$

folgt

$$D(qp_1)^2 + sp_1{}^2 = (pp_1)^2$$

und da

$$p_1{}^2 = Dq_1{}^2 + s_1,$$
$$D(qp_1)^2 + sDq_1{}^2 + ss_1 = (pp_1)^2;$$

da ferner

$$s = p^2 - Dq^2,$$
$$D(qp_1)^2 + p^2q_1{}^2D - D^2q^2q_1{}^2 + ss_1 = (pp_1)^2,$$
$$D(qp_1)^2 + (pq_1)^2D + ss_1 = (pp_1)^2 + D^2q^2q_1{}^2$$
$$\pm 2Dpp_1qq_1 = \pm 2Dpp_1qq_1$$
$$\overline{D(qp_1 \pm q_1p)^2 + ss_1 = (pp_1 \pm Dqq_1)^2.}$$

Beweis.

$$Du^2 = D(p^2q_1{}^2 \pm 2pp_1qq_1 + q^2p_1{}^2)$$
$$t^2 = pp_1 \pm 2Dpp_1qq_1 + D^2q^2q_1{}^2.$$
$$\overline{Du^2 - t^2 = p^2(Dq_1{}^2 - p_1{}^2) + Dq^2(p_1{}^2 - Dq^2)}$$
$$= -(p^2 - Dq^2)(p_1{}^2 - Dq_1{}^2)$$
$$= -ss_1.$$

Mit Hilfe dieser Regel kann man nun aus einer Auflösung der Gleichung $Du^2 + s = t^2$ eine solche der Gleichung $Du^2 + s^2 = t^2$ finden. Denn aus

$$Dq^2 + s = p^2,$$
$$Dq^2 + s = p^2$$

folgt

$$D(qp \pm qp) + s^2 = (p^2 \pm Dq^2)^2.$$

Es sind nur die oberen Zeichen zu brauchen und man erhält

$$Q = 2pq, \; P = p^2 + Dq^2$$

als Auflösung der Gleichung

$$Du^2 + s^2 = t^2.$$

§ 86. ......composition serves to deduce roots for additive unity from those wich answer to the additive four and two.

1. Im Falle $s = 1$ liefert somit

$$Q = 2pq, \; P = p^2 + Dq^2$$

eine neue Auflösung der Gleichung $t^2 - Du^2 = 1$, wenn man eine, p, q kennt.

2. Im Falle $s = -1$ erhält man aus einer Auflösung der Gleichung $t^2 - Du^2 = -1$ eine solche für $t^2 - Du^2 = 1$.

3. Im Falle $s = \pm 2$ endlich findet man mit Hilfe der gleichen Formel aus einer Lösung für $t^2 - Du^2 = \pm 2$ eine Auflösung der Gleichung $t^2 - Du^2 = 4$.

Von hier aus gelangt man aber leicht zu einer Lösung für $t^2 - Du^2 = 1$. Denn aus

$$Dq^2 \pm 2 = p^2$$

folgt

$$D4p^2q^2 + 4 = (p^2 + Dq^2)^2$$

also, da alles ganzzahlig,

$$Dp^2q^2 + 1 = \left(\frac{p^2 + Dq^2}{2}\right)^2.$$

§ 79. Let the additive divided by the square of an assumed number be a new additive; and the roots divided by that assumed number, will be the corresponding roots. Or the additive being multiplied [by the square] the roots must in like manner by multiplied [be the number put].

Section II. § 83—86. Rule for the cyclic method (Colebrooke. p. 175). Making the „least" and „greatest" roots and additive.....

a dividend additive and divisor let the multiplier be thence found.

The square of that multiplier being subtracted from the given coefficient, or this coefficient being subtracted from the square (so as the remainder be small)

the remainder, divided by the original additive is a new additive, wich is reversed if the subtraction (of the squarre) be from the coefficient. The quotient corresponding to the multiplier (and found with is) will be the „least" root, whence te greatest root may by deduced.

Auflösung von $Du^2 + 1 = t^2$.

Man wähle 2 nicht gemeinteilige Zahlen p, q, so dass

$$Dq^2 + s = p^2.$$

Dabei sieht man zu, dass s möglichst klein wird; doch ist dies nur wünschenswert, damit das Verfahren bald zum Ziele führe, nicht jedoch notwendig.

Nun bestimmt man die Zahlen r, für welche $q_1 = \pm \frac{p + qr}{s}$ eine ganze Zahl wird. Dies geht, da p und q nicht gemeinteilig sind, und wurde von den Indern nach der mit unserem Kettenbruchverfahren identischen Cuttaca oder Zerstäubungsmethode ausgeführt.

Man wählt denjenigen Wert r, für welchen $\pm (r^2 - D)$ möglichst klein wird.

Dann wird, so behaupten die Inder, $s_1 = \pm \left(\frac{r^2 - D}{s}\right)$ eine ganze Zahl und

$$Dq_1{}^2 + s_1{}^2 = \left(\frac{pq_1 - 1}{q}\right)^2 = p_1{}^2.$$

Der Beweis für diese Behauptung fehlt bei Bhaskara; man kann ihn aber nach Hankel wie folgt ergänzen. Da

$$q_1 = \frac{p + qr}{s} = \text{num. integ.}$$

folgt ganzzahlig

$$q_1 s = p + qr,$$

da

$$s = p^2 - Dq^2,$$

ferner

$$q_1(p^2 - Dq^2) = p + qr,$$
$$p(pq_1 - 1) = q(r + Dqq_1).$$

Da nun gemäss der gemachten Voraussetzung p und q nicht gemeinteilig[1]) sind, wird

$$\frac{pq_1 - 1}{q} = \text{num. integ.}$$

Nun ist aber

$$r = \frac{q_1 s - p}{q},$$

also

$$r^2 - D = \frac{(q_1 s - p)^2 - Dq^2}{q^2}$$
$$= \text{num. integ.}$$

und da $Dq^2 = p^2 - s$

somit

$$\frac{r^2 - D}{s} = \frac{q_1{}^2 s - 2pq_1 + 1}{q^2}$$
$$= \text{num. integ.; endlich}$$

$$\text{num. integ.} = \frac{r^2 - D}{s}$$

$$= \frac{r^2 - D}{p^2 - Dq^2} = \frac{q_1{}^2 s - 2pq_1 + 1}{q^2}$$

$$= \frac{q_1{}^2(p^2 - Dq^2) - 2pq_1 + 1}{q^2}.$$

$$= \left(\frac{pq_1 - 1}{q}\right)^2 + Dq_1{}^2,$$

oder

$$s_1 = p_1{}^2 + Dq_1{}^2, \text{ wo } p_1 = \frac{pq_1 - 1}{q}.$$

This method mathematicians call that of the circle. This are

Nach der angegebenen Weise soll man fortfahren, immer neue

1) Der Ausdruck wird angewendet nach einem Vorschlage H. Schapiras (deutsche Bearbeitung von Tschebyscheff, Theorie der Kongruenzen, Berlin 1889), auf den Hofrat Prof. Dr. Cantor mich aufmerksam gemacht hat.

integral roots found with four two or one [or other number[1])] for additive and composition serves to deduce roots for additive unity from those wich answer to the additive four and two (or other number).

p_k, q_k, s_k zu bilden, bis einmal ein s gleich ± 1, ± 2 oder ± 4 wird, alsdann geben die früher aufgeführten Hilfsbemerkungen die gesuchte Lösung, resp. eine Lösung der verlangten Art.

Es fehlt allerdings, das ist hervorzuheben, der Nachweis, dass das Verfahren immer zum Ziele führt, resp., dass immer einmal einer der Additiven ± 1, ± 2 oder ± 4 auftreten muss.

§ 87. Vi'ja-Gan'ita. Chap. III. Section II.

Beispiele: Bei Bhaskara finden sich auch Beispiele für das „cyklische" Verfahren und zwar für die Fälle $D = 61$, $D = 67$, welche beide rasch und bequem gelöst werden, trotzdem gerade der Fall $D = 61$ auf sehr grosse Zahlen führt. Für $D = 67$ zum Beispiel fällt die Berechnung folgendermassen aus.

Ganzzahlig zu lösen ist:

$$67u^2 + 1 = t^2,$$

man wähle die naheliegenden Zahlen

$$q = 1,\ p = 8,$$

so dass

$$67 \cdot 1^2 - 3 = 8^2,$$

$$q_1 = \pm \frac{8 + r}{3};$$

r ist so zu wählen, dass

$$r^2 - D = r^2 - 67$$

möglichst klein wird, also $r = 7$,

Zum Vergleich setze ich die Berechnung nach dem gewöhnlichen Verfahren daneben.

$$\sqrt{67} = 8 + \frac{1}{\alpha};\ \alpha = \frac{\sqrt{67}+8}{3} = 5 + \frac{1}{\beta}$$

$$\frac{1}{\beta} = \frac{\sqrt{67}-7}{3};\ \beta = \frac{\sqrt{67}+7}{6} = 2 + \frac{1}{\gamma}$$

$$\frac{1}{\gamma} = \frac{\sqrt{67}-5}{6};\ \gamma = \frac{\sqrt{67}+5}{7} = 1 + \frac{1}{\delta}$$

$$\frac{1}{\delta} = \frac{\sqrt{67}+2}{7};\ \delta = \frac{\sqrt{67}-2}{9} = 1 + \frac{1}{\varepsilon}$$

$$\frac{1}{\varepsilon} = \frac{\sqrt{67}-7}{9};\ \varepsilon = \frac{\sqrt{67}+7}{2} = 7 + \frac{1}{\zeta}$$

1) Die beiden Zusätze in den Klammern rühren vom Kommentator CRĬSŃ her. Sie sind jedoch überflüssig und unrichtig.

$$\frac{1}{\zeta} = \frac{\sqrt{67}-7}{2};\ \zeta = \frac{\sqrt{67}+7}{9} = 1 + \frac{1}{\eta}$$

etc., die Periode heisst also 8, 5, 2, 1, 1, 7, 1, 1, 2, 5, 16 etc.; hieraus bekommt man die Näherungsbrüche

$$\frac{8}{1};\ \frac{14}{5};\ \frac{90}{11};\ \frac{131}{16};\ \frac{221}{27};\ \frac{1678}{205};$$

$$\frac{1899}{232};\ \frac{3577}{437};\ \frac{9053}{1106};\ \frac{48842}{5967};\ \text{etc.}$$

Der letzte liefert die gesuchte Lösung

$$67\,(5967)^2 + 1 = (48842)^2.$$

daher

$$s_1 = -\frac{r^2 - D}{5} = 6;\ q_1 = -5;\ p_1 = 41,$$

$$\underline{67 \cdot (5)^2 + 6 = 41^2.}$$

$$q_2 = \frac{41 + 5r_2}{6};\ r_2 = 5;$$

$$s_2 = \frac{r_2{}^2 - 67}{6} = -7.$$

$$q_2 = 11;\ p_2 = 90,$$

$$\underline{67 \cdot (11)^2 - 7 = (90)^2.}$$

$$q_3 = -\frac{90 + 11r_3}{7};\ r_3 = 9;$$

$$s_3 = \frac{r_3{}^2 - 67}{-7} = -2.$$

$$q_3 = -27,\ p_3 = -221,$$

$$\underline{67 \cdot (27)^2 - 2 = (221)^2.}$$

Nach der Hilfsbemerkung[1]) ist nun

$$67\,(2 \cdot 27 \cdot 221)^2 + 4$$
$$= (221^2 + 67 \cdot 27^2)^2,$$

$$67\,(11934)^2 + 4 = (97684)^2,$$

also

$$\underline{67\,(5967)^2 + 1 = (48842)^2.}$$

Neben dieser systematischen Methode benutzten auch die Inder schon verschiedene Kunstgriffe, unter anderem die Verwendung gebrochener Zahlen. Die Formel, welche sie zur Auflösung der Gleichung $t^2 - Du^2 = 1$ in gebrochenen Zahlen angeben, möge hier noch ihren Platz finden, weil sie genau die gleiche ist, auf welche Wallis und Brouncker zuerst kamen, als ihnen Fermat die Aufgabe vorgelegt hatte.

---

1) Siehe S. 20.

Vi'ja-Gan'ita. Chap. III. Section I. § 80 und 81.

Or divide the double of an assumed number by the difference between the square of that assumed number and the given coefficient and let the coefficient be taken for the least root, when one is the additive quantity and from that find the greatest root. Here (the solutions are) infinite as well from (variety of) assumptions, as from diversity of composition.

Ich gebe Regel und Beweis in der Fassung des Kommentators.

Es gilt $t^2 - Du^2 = 1$ in rationalen Brüchen zu lösen. Man setzt

$$u = 2\beta,$$
$$D4\beta^2 + b^2 = t^2,$$
$$b^2 = (D - \beta^2)$$

gesetzt, giebt

$$D4\beta^2 + (D - \beta^2)^2 = (D + \beta^2)^2,$$
$$D\left(\frac{2\beta}{D - \beta^2}\right)^2 + 1 = \left(\frac{D + \beta^2}{D - \beta^2}\right)^2.$$

Oder nach § 79 etwas anders und einfacher so: aus

$$Dq^2 + C = p^2,$$

wo p, q beliebig

$$\text{und } Dq^2 + C = p^2$$

folgt

$$D(2pq)^2 + C^2 = (p^2 + Dq^2)^2,$$

also

$$D\left(\frac{2pq}{C}\right)^2 + 1 = \left(\frac{p^2 + Dq^2}{C}\right)^2.$$

Doch das sind nur gelegentliche Kunstgriffe, während die „cyklische" Methode mit Recht als Methode bezeichnet wird. Hankel bemerkt[1]: „Die Methode ist über alles Lob erhaben. Sie ist sicher das Feinste, was in der Zahlenlehre vor Lagrange geleistet worden ist! Sie ist merkwürdigerweise genau dieselbe, welche Lagrange in seiner 1767 erschienenen Abhandlung[2] vortrug und erst nachträglich auf den Kettenbruchalgorithmus für $\sqrt{D}$ reduzierte, den Euler im Jahre 1759 auf das Problem angewandt hatte."[3] „Man sollte die Gleichung zur Erinnerung an diese merkwürdige Anticipation einer im Oriente hochgefeierten Entdeckung in Zukunft die indische nennen." Es fehle der cyklischen Methode nichts als der Beweis, der erst Lagrange anderthalb Jahrtausende später gelungen sei.

1) Hankel, Zur Geschichte etc. Leipzig 1874. S. 200.

2) Lagrange, Sur la solution des probl. indet. du IIième degré. 1768! Mém. de l'academie de Berlin. Tome 23. Ges. Werke. Bd. II. p. 377.

3) Euler, Comm. arithm. collectae I. p. 316.

Alles das setzt indes vor allem voraus, dass sich unsere Methode, wie sie hier vorgetragen ist, wirklich mit der indischen deckt. Darüber herrscht nicht völlige Übereinstimmung. Cantor[1]) z. B. setzt das Verfahren etwas anders auseinander und sagt dann:

„Allerdings wird das indische Verfahren nicht stets zum Ziele führen, namentlich nicht nach ganz vorschriftsmässigen Regeln die Wurzeln der Gleichung $Du^2 + b = t^2$ finden lassen.“

Ich möchte jedoch der Hankelschen Darlegung den Vorzug geben. Denn wie unser obiger Vergleich mit dem Original zeigt, benutzt sie nichts, was sich nicht wirklich bei den Indern findet; die Methodik passt vorzüglich auf die Beispiele, und endlich wird der Vergleich mit dem Lagrangeschen Verfahren zeigen, dass die Auflösungsmethode in der That richtig ist und stets zum Ziele führen muss.

Es wäre, schon des Vergleichs mit den Griechen wegen, interessant, zu wissen, woher die Inder die Anregung zur Behandlung der Gleichung $t^2 - Du^2 = 1$ empfingen, wie sich die Kenntnis des Problems entwickelte und wie man zu der cyklischen Auflösung gelangte. Leider ist man in dieser Hinsicht gänzlich auf Vermutungen angewiesen.

Hankel betrachtet die Auflösung als eigenste Leistung der Inder. Dieselben seien vielleicht durch die Reduktion der allgemeinen unbestimmten Gleichung zweiten Grades, welche ihnen ja bekannt war, auf die Aufgabe gekommen und unmittelbar aus ihr heraus auf die Lösung, etwa auf dem Wege, welchen Hankel l. c. p. 201 angiebt.

Ja, selbst die griechische unbestimmte Analytik Diophants soll nach demselben Autor auf die indische Mathematik zurückzuführen sein.[2])

Dem gegenüber vertritt Cantor den Standpunkt,[3]) dass umgekehrt griechische Anregung bei den Indern gewirkt habe, nur gerade die unbestimmte ganzzahlige Analytik sei ihr eigenstes Eigentum. Vielleicht seien astronomische Fragen, vielleicht das Studium magischer Quadrate die Veranlassung zur Ausbildung der Theorie der ganzzahlig zu lösenden Aufgaben gewesen.

Das entgegengesetzte Extrem wie Hankel verteidigt Tannery.[4])

1) Cantor, Vorlesungen über Geschichte etc. Leipzig 1880. I_1. S. 536 u. f. I_2. 591 u. f.

2) Hankel, Zur Geschichte der Mathematik im Altertum und Mittelalter. Leipzig 1874. S. 204.

3) Cantor, Vorles. über Geschichte der Math. Bd. I_1. Leipzig 1880. S. 533. I_2. S. 556 u. f.

4) P. Tannery, Sur la mesure du cercle d'Archimède. Mém. de la soc. des sc. phys. et nat. de Bordeaux. Bordeaux 1882. IIième sér. Tome III. p. 325.

Er glaubt auch in der Arithmetik der Inder einen griechischen Einfluss und griechische Anregung zu erkennen und ist geneigt, selbst in der „cyklischen“ Methode nur eine Abart des Verfahrens zu sehen, nach welchem die Griechen die Gleichung $t^2 - Du^2 = 1$ rechnerisch lösten. Tannery zeigt in der That, dass man von der Aufgabe, aus einem gegebenen Näherungswert einer Quadratwurzel nach griechischer Manier einen genaueren abzuleiten, durch einfache Schlüsse zu der indischen Methode gelangen kann.

Ich bin ausser stande, zwischen diesen drei Ansichten eine Entscheidung zu treffen. Am ehesten möchte ich mich der von Cantor anschliessen, da sie mir am wenigsten den Boden des geschichtlich festgestellten zu verlassen scheint und zu der unzweifelhaften Originalität und Systematik der Inder am besten passt.

Doch berührt diese Streitfrage in keiner Weise die Thatsache, dass die Inder jedenfalls um 600 n. Chr. im Besitz einer Methode zur ganzzahligen Lösung der Gleichung $t^2 - Du^2 = 1$ waren, welche, der Sache nach eine Kettenbruchmethode,[1]) nichts zu wünschen übrig liess, als den Beweis, dass sie auch stets zum Ziele führt.

---

1) Hierzu auch Günther, Die quadratischen Irrationalitäten etc. S. 40, § 13.

II. Teil: Von Fermat bis Lagrange.

§ 1. Fermat.[1])

Die Araber, welche im Abendlande das Erbe der griechischen Mathematik antraten, haben sich, wie es scheint, nicht mit der Gleichung $t^2 - Du^2 = 1$ beschäftigt. So geriet bei den europäischen Völkern auch das, was die Griechen vielleicht einst in Bezug auf die ganzzahlige Lösung unserer Gleichung ermittelt hatten, völlig in Vergessenheit.

Fermat bleibt der ungeschmälerte Ruhm, das Problem neu entdeckt und in der Arithmetik eingebürgert zu haben.

Wie und wann er dazu gekommen ist, sich mit der Gleichung $t^2 - Du^2 = 1$ zu beschäftigen, lässt sich nicht feststellen. Vielleicht war die Reduktion der allgemeinen unbestimmten Gleichung zweiten Grades der Anlass dazu, obwohl es dann merkwürdig ist, dass sich in seinen Bemerkungen zu Diophant nichts davon findet. Vielleicht besteht ein Zusammenhang mit seiner Beschäftigung mit Theon Smyrnäus.[2]) Freilich haben alle derartigen Vermutungen wenig Wert bei einem Manne, der in seinen mathematischen Spekulationen so entlegene Wege wandelte, wie Fermat.

Gleich das erste Mal, wo wir dem Problem bei Fermat begegnen, wird es in seiner vollsten Allgemeinheit ausgesprochen; es wird, was bisher noch niemals geschehen, der Beweis verlangt, dass es stets Zahlen

---

1) Der folgende Teil war ebenso wie das Meiste dieser ganzen Schrift bereits Anfang 1898 fertiggestellt und ist damals in den Händen verschiedener Herren zu Bonn, insbesondere Herrn Geh. Prof. Dr. Lipschitz gewesen, ehe mir der Aufsatz von Wertheim [Pierre Fermats Streit mit John Wallis. Ein Betrag zur Geschichte der Zahlentheorie. Zs. Math. Phys. 44. Suppl. 14. Abhandlungen zur Geschichte der Mathematik 9 (Festschrift für M. Cantor) 1899 (S. 557 bis 576)] bekannt war.

2) Vergl. Recherches sur les manuscrits de Pierre de Fermat suivies de fragments inédits de Bachet et de Malebranche par C. Henry. Bulletino de bibliografia e de storia delle scienze matematiche e fisiche. — Pubblicato da B. Boncompagni. Tomo XII. Roma 1879. p. 490.

gebe, welche der Forderung $t^2 - Du^2 = 1$ genügen, und endlich zeigt die Wahl der Beispiele ($D = 61, 109$), deren Berechnung ohne systematisches Verfahren auch Fermat kaum geglückt sein dürfte, selbst wenn man die merkwürdige Geschicklichkeit der damaligen Mathematiker im Behandeln und Übersehen grosser Zahlen in Anschlag bringt, dass Fermat im Besitze eines Verfahrens sein musste, um sich über die Grösse der kleinsten Lösungen für gegebenes D zu orientieren.

Die Stelle, auf welche wir uns beziehen, steht in einem Briefe Fermats an Frenicle[1]) aus dem Februar 1657.[2]) Sie lautet:

„Tout nombre non quarré est de telle nature, qu'on peut trouver infinis quarrés, par lesquels si vous multipliez le nombre donné et si vous ajoustez l'unité au produit, vienne un quarré" Beispiele $D = 3$, $u^2 = 1, 16$.

„Je vous demande une reigle gènèrale pour estant donné un nombre non quarré trouver des quarrés, qui, multipliés par le dit nombre donné, en adjoustant l'unité fassent des nombres quarrés. Quel est par exemple le plus petit quarré qui, multipliant 61 en prenant l'unité fasse un quarré? Item, quel est le plus petit quarré qui multipliant 109 et prenant l'unité fasse un quarré? Si vous ne m'envoyez pas la solution générale envoyez-moy la particulière de ces deux nombres que j'ay choisis des plus petits, pour ne vous donner pas trop de peine.[3]) Apres que j'auray receu vostre response, je vous proposeray quelque autre chose. Il paroist, sans le dire, que ma proposition n'est que pour trouver des nombres entiers, qui satisfassent à la question, car en cas de fractions le moindre arithemétieien en viendroit à bout."

Zur gleichen Zeit forderte Fermat alle lebenden Mathematiker zu einem arithmetischen Wettkampf heraus;[4]) unter den Aufgaben, welche er hierzu in seinem zweiten „Défi"[5]) stellt, befindet sich auch unser Problem. Es heisst, nachdem in der Einleitung unter Hervorhebung des Gegensatzes zu Diophant ganzzahlige Lösungen verlangt worden sind:

---

1) Bernard Frenicle de Bessy (1605—1675) angestellt in Paris am Münzamte, war Mathematiker aus Liebhaberei und wurde von seinen Zeitgenossen als solcher hochgeschätzt.

2) Oeuvres de Fermat. Tome IIième. Paris 1894. S. 333. Brief Nr. 80. — Commercium epistolicum. Nr. 33. — Correspondance de Huyghens. Nr. 372.

3) Fermat hat sich hier offenbar mit Frenicle einen Scherz erlaubt. Denn 109 liefert von allen Werten $D = 1$ bis $D = 139$ die grössten Zahlen.

4) Man vergleiche über den Grund und die Vorgeschichte dieses Wettkampfes den S. 29 citierten Aufsatz Wertheims. § 1—3.

5) Secon Défi de Fermat, Aux Mathématiciens. Févr. 1657. — Oeuvres de Fermat. Bd. II. Paris 1894. p. 334. Commercium epistolicum. Nr. 8.

„Quibus, ut praeviam lucem praeferamus theorema seu problema sequens aut demonstrandum aut construendum proponimus; hoc autem si invenerint, fatebuntur, huiusmodi quaestiones nec subtilitate nec difficultate nec ratione demonstrandi celebrioribus ex geometria esse inferiores.“ „Dato quovis non quadrato, dantur infiniti quadrati, qui in datum numerum ducti adscita unitate conficiant quadratum.“ „Exemplum $D = 3$, $u^2 = 1, 16$ et loco 1 et 16 possunt infiniti quadrati idem praestantes inveniri, sed canonem generalem dato quovis numero non quadrato inquirimus. Quaeratur, verbi gratia, quadratus qui ductus in 149 aut 109 etc. adscita unitate conficiat quadratum.“

Wir werden sehen, wie diese Herausforderung verbreitet wurde und wie die darin gestellte Aufgabe nach längeren Missverständnissen und vergeblichen Versuchen in England durch Wallis[1]) und Brouncker[2]) ihre Lösung fand, obwohl auch diesmal der Beweis nicht glückte, dass für jedes D das Problem überhaupt lösbar sei.

Wie Fermat über die schliessliche Lösung durch Wallis und Brouncker urteilte, lässt sich nicht sicher ermitteln. In einem Brief vom 19. Juni 1658 erkennt er die englische Methode vollständig an und sagt:[3])

„Ill. viros . . . . quaestionum numericarum a me propositarum solutiones tandem dedisse legitimas libens agnosco, imo et gaudeo . . . .“ „Verum . . . . fatentur Galli propositis quaestionibus satisfecisse Anglos,“ während es in der „Relation des nouvelles découvertes etc.“ [4]) vom August 1659 heisst:

„J'avoue que M. Frenicle a donné diverses solutions particulières et M. Wallis aussi, mais la démonstration générale se trouvera par la „descente“ dûment et proprement appliquée: ce qui je leur indique, afin qu'ils ajoutent la démonstration et construction générale du théorème (!) et du problème aux solutions singulières qu'ils ont données.“

Ich werde auf diesen Punkt noch bei der Auseinandersetzung der Wallisschen Methode einzugehen haben.

---

1) John Wallis (1616—1703), seit 1649 Professor der Geometrie in London.

2) William Brouncker, Lord (1620—1684). Seit 1660 Kanzler und Grosssiegelbewahrer der Königin; seit 1662 Präsident der Royal Society. Ich folge in der Schreibweise Brouncker im Comm. ep und bei Wertheim.

3) Fermat, Oeuvres. Bd. II. Paris 1894. p. 402. Bd. III. Paris 1896. p. 598. p. 602. — Commercium epistolicum. I. Ausgabe Anhang. II. Ausgabe Nr. 47.

4) Fermat, Oeuvres tome II. Paris 1894. p. 431. No. 101. Fermat an Carcavi. Correspondance de Huyghens. No. 651.

Der letztgenannte berühmte Brief an Carcavi ist es auch, in welchem Fermat ausdrücklich behauptet, unser Problem mit Hilfe der „descente" streng gelöst zu haben, er sagt:[1])

„4. Celle (sc. question) que j'avois proposée à M. Frenicle et autre est d'aussi grande ou même plus grande difficulté (sc. que le théorème: Tout nombre est quarré ou composé de deux, de trois au de quatre quarrés): Tout nombre non quarré est de telle nature qu'il y a infinis quarrés qui, multipliant le dit nombre font un quarré moins 1. Je la démontre par la „descente" appliquée d'une manière tout particulière."

Bezüglich der Andeutungen über das „Descente" genannte Verfahren muss ich mich darauf beschränken, auf die in jeder Hinsicht hochinteressante und merkwürdige „Relation" zu verweisen.[2])

Es ist eine alte und meist zu Ungunsten Fermats entschiedene Streitfrage, ob er die Methoden und Beweise wirklich besessen, deren er sich rühmt. Ohne hier darauf eingehen zu wollen, möchte ich doch hervorheben, wie die ganze Fassung des eben citierten Briefes, der Passus mit dem unrichtigen Satz von der nur Primzahlen darstellenden Formel im Verein mit der strengen Beurteilung eigner und fremder Beweisversuche (gerade bei unserem Problem), so gar nicht dazu passen will, dass Fermat blosse „Induktion" für einen vollgültigen Beweis gehalten und allein durch sie seine tiefsinnigen Sätze gefunden haben soll.[3])

Es bleibt noch zu erwähnen, dass auch das Wallissche Lösungsverfahren Fermat zugeschrieben worden ist. Dahingehende Bemerkungen finden sich bei Lagrange,[4]) Gauss[5]) und — offenbar im Anschluss an letzteren — bei Bachmann.[6]) Alle stützen sich auf eine Angabe Ozanams. Die Stelle lautet:[7])

---

1) Fermat, Oeuvres T. 2. p. 433.

2) Hierzu Cantor, Vorl. über Geschichte der Math. Bd. II_1. Leipzig 1890. S. 708. II_2. S. 715.

3) Siehe auch Dirichlet, ges. Werke. Bd. I. S. 197! Untersuchungen über die Theorie der quadratischen Formen.

4) Lagrange, Oeuvres. Bd. VII. Paris 1877. p. 157. Additions aux élémens d'algèbre d'Euler. § VIII. No. 84. Zeile 5 (1774).

5) Gauss, Disqu. arith. art. 202. Werke Bd. I. art. 202. 6. Zeile.

6) P. Bachmann, Zahlentheorie. II. Bd. 8⁰. Leipzig 1892. S. 189.

7) Nouveaux élémens d'algèbre ou principes généraux pour résoudre toutes sortes de problème de mathématique, par M. Ozanam (M. heisst hier Monsieur, der Verfasser hiess Jacques) Professeur de Mathématique. 3. Bd. 8⁰. Amsterdam b. George Gallet. 1702. Buch III. Question XXVI. p. 509. Genaueres über Ozanam in dem Seite 29 citierten Aufsatz von Henry. S. 558, ausserdem Montucla I. S. 324. — Cantor, Geschichte der Mathematik. III. Bd. I. Abt. Leipzig 1894.

„.... et que d'ailleurs la solution est toujours possible en nombres entiers pour quelque nombre entier donné que ce soit pourvû qu'il ne soit pas quarré, nous enseignerons ici une règle générale pour résoudre cette question, qui est de M. de Fermat.“

Möglicherweise ist die Zweideutigkeit von „qui“ an dem Missverständnis schuld. Sonst liegt jedenfalls ein Irrtum Ozanams vor, der, wie man aus seinen „Récréations“ sehen kann, bei aller Gelehrsamkeit höchst unkritisch verfuhr. Denn die von ihm referierte Methode stimmt bis auf die Beispiele wörtlich mit der unzweifelhaft von Wallis und Brouncker herrührenden überein.

Angesichts der Verdienste Fermats um die Gleichung $t^2 - Du^2 = 1$ wäre es wohl, so scheint mir, eine Pflicht der Gerechtigkeit, die Aufgabe zu Ehren ihres Entdeckers die Fermatsche zu nennen und endlich den durch nichts als das Herkommen gerechtfertigten Namen der Pellschen Gleichung fallen zu lassen.[1])

S. 98) erwähnt nur Jacques Ozanam, récréations mathématiques. 4 Bd. Paris 1749 und einen Aufsatz im Journal des sçavans von 1680. Ausser diesen Schriften und der zuerst genannten rührt von Ozanam noch her: Cours de mathématique qui comprend toutes les parties les plus utiles et les plus nécessaires à un homme de guerre et à tous ceux pui se veulent perfectionner dans cette science. V Bd. par M. Ozanam etc. nouv. éd. rév. et corr. A Paris chez Jean Jombert 1697. Nach den kurzen Citaten bei Lagrange und Gauss konnte jede dieser Schriften gemeint sein.

1) Die Bezeichnung „Pellsche“ Gleichung rührt von Euler her, welcher in dem Aufsatz „de usu novi algorithmi in problemate „„Pelliano““ solvendo. (Comm. arith. coll. I. p. 316) ausdrücklich sagt: „...atque hoc est illud problema olim quidem maxime celebratum a solutionis ingeniosissimae auctore Pellianum vocatum......... etiamsi solutio Pelliana huius problematis set elegantissimae...“ und in der Algebra Artikel 98: „Hierzu hat ein gelehrter Engländer Namens Pell eine sehr sinnreiche Methode erfunden etc..“ Nach der Angabe von Hankel (Zur Geschichte der Mathematik im Altertum und Mittelalter. Leipzig 1874. S. 203) soll Euler zu seinem Irrtum durch die englische Übersetzung der deutschen Algebra Joh. Heinr. Rahns (1622—1676) gekommen sein, die Pell durch Brouncker anfertigen liess, und in welcher die Wallissche Lösung der Gleichung $t^2 - Du^2 = 1$ im Anhang wieder abgedruckt worden sei, ohne Angabe des Autors. Das einzige Exemplar des, wie es scheint, selten gewordenen Werkes, das ich erhalten konnte, befindet sich in Göttingen und führt den Titel: An Introduction to algebra translated out of the High-dutch into English by Thomas Brancker, M. A. much Altered and Augmented by. D. P. (soll wohl heissen Pell) also: a Table of odd numbers less than one hundred Thousand shewing those that are incomposit and resolving the rest into their Factors or coefficients. Suppurated by the same Th. Brancker, London. Printed by W. G. for Moses Pitt at the white-Hart in Little Britain. 4⁰. 1668. — In der vom 22. April 1668 datierten Vorrede heisst es das Original sei: Algebra Rhonii, Germanice; Tiguri apud Bodmerum 1659. Die

Wollte man freilich die ersten Entdecker ehren, so müsste man die Gleichung, wie Hankel will,[1] die „indische“ oder gar die Archimedische nennen. Doch blieb die Entdekung durch die Griechen und Inder unfruchtbar, während die Fermatsche in gewissem Sinne epochemachend wurde und bis zum heutigen Tage fortwirkt.

§ 2. Frenicle, Wallis und Brouncker.

Die zweite Herausforderung Fermats vom Februar 1657 gelangte zuerst zu seinen Pariser Freunden und wurde von diesen nach England und Holland weitergeschickt. Sie wurde in Paris von Frenicle, in England von Wallis und Brouncker aufgenommen.

Frenicle, der damals in Frankreich[2]) und sogar bei Fermat[3]) als Zahlentheoretiker im höchsten Ansehen stand, fand noch[4]) am selbigen

---

Übersetzung (resp. Zusätze) rührten von Seite 100 ab von P. (soll wohl heissen Pell) her. Trotzdem das Exemplar aus Göttingen keine Anzeichen von Unvollständigkeit an sich trug, enthielt es die Lösung der Gleichung $t^2 - Du^2 = 1$ nicht. Ich möchte jedoch nicht, auf Grund dieses vielleicht zufälligen Umstandes die Darlegungen Hankels anzweifeln. [Man vergl. hierzu M. Curtze in der Bibliotheca Mathematica 1901. p. 143, wo mitgeteilt wird, die Originalhandschrift werde in der Züricher Stadtbibliothek aufbewahrt und der Verfasser der Algebra nenne sich, wie es auch die englische Übersetzung angiebt, Rhonius.] Während Gauss Lagrange und Legendre die Bezeichnung „Pellsche“ Gleichung nur unter Berufung auf die Autorität Eulers bringen, bedient sich Dirichlet derselben rückhaltlos in seinen Schriften und sagt z. B. (ges. Werke l, p. 222): „Die Aufgabe .... beschäftigte Pell und Lord Brouncker deren Lösungen etc.“ Die Autorität Dirichlets und Eulers wird dann den Gebrauch der Bezeichnung Pellsche Gleichung allgemein gemacht haben. Hierzu auch Smith, Report on the Theory of Numbers 1861. Coll. Papers. Bd. I. p. 192. Oxford 1894. Man vergl. hierzu die Anm. p. 562 des schon oft zitierten Aufsatzes von Wertheim. Vergl. p. 48.

1) Hankel, Zur Geschichte der Mathematik im Altertum und Mittelalter. Leipzig 1874. p. 203.

2) Commercium epistolicum, ed. John Wallis. Oxford 1658 oder: Opera D. Wallisii. Oxford 1693. Bd. II abgedruckt und übersetzt in Fermat, Oeuvres. Tome III. Paris 1896. p. 399 u. f. Brief Nr. 25. p. 529. An letztgenannter Stelle sagt Digby: „Or quoiqu'il [Frenicle] ne soit, à son idée qu'un très mince mathématicien, aujourd'hui pour la partie qui concerne les nombres, toute la France (même M. Roberval et M. de Fermat) le reconnait comme le maitre supérieur aux autres à une énorme distance.“

3) Commercium ep. l. c. Nr. XXXVII. Fermat, Oeuvres. Bd. II. Paris 1894. p. 377 schreibt Fermat an Digby: „Mais ma question ‚en entiers‘ est si fort au dessus de ces petites règles ‚de trivio‘, que M. Frenicle l'a jugée digne de l'occuper, et c'est tout dire.“

4) Commercium ep. l. c. No. VI. Fermat, Oeuvres. Tome III. Paris 1896. p. 411.

Tage, wo ihm der[1]) Brief Fermats überbracht wurde, einige spezielle Lösungen und gab bald darauf ein leider verloren gegangenes kleines lateinisches Buch heraus, in welchem er ohne genauere Angaben über die Methode der Berechnung eine Tabelle der kleinsten Auflösungen unserer Gleichung für alle Werte von $D = 1$ bis $D = 150$ gab und zugleich gegen Wallis und Brouncker polemisierte.[2])

Worin seine Berechnungsmethode bestand, lässt sich nicht ermitteln. Wallis erzählt, Frenicle habe sie Huyghens gezeigt;[3]) sie sei aber zur Berechnung schwierigerer Beispiele zu kompliziert gewesen, so dass jener, wie er selbst in dem erwähnten Büchlein erzähle, die Auflösung der Gleichung $t^2 - 109\,u^2 = 1$ erst von Fermat bekommen habe.[4]) Selbst hat auch Wallis die Methode Frenicles nicht zu Gesicht bekommen; er kennt nur Frenicles „Traité" und die Kritik, die er an demselben ausübt, lässt fast vermuten, dass auch Frenicles Verfahren nur in einer Art systematisiertem Ausprobieren bestand.[5])

In ähnlichem Sinne spricht sich auch Fermat in dem Seite 31 citierten Briefe an Carcavi aus.

Trotz des grossen Rufes, dessen sich Frenicle erfreute und trotz der richtigen Auffassung des Wesens der Aufgabe, die er in der Korrespondenz mit Wallis an den Tag legt, wird man, glaube ich, doch schliessen müssen, dass jener sich nicht im Besitze einer wirklich allgemeinen Lösungsmethode, geschweige denn eines strengen Beweises der Lösbarkeit befunden habe.

Mit mehr Erfolg versuchten sich Wallis und Brouncker an dem Problem. Anfangs freilich missverstanden sie es vollständig und glaubten mit einer Formel zur rationalen Auflösung der Gleichung

---

1) Vergl. weiter oben S. 30 und 31.

2) Commercium epistolicum, l. c. ep. No. XVIII. Fermat, Oeuvres. Bd. III. p. 480 und 488. Wallis spricht von einem „Traité de M. Frenicle sur les problèmes de Fermat". Ferner Brief Nr. XXXII des Comm. epist. Fermat, Oeuvres. Tome III. Paris 1896. p. 554, ebenso Cantor, Geschichte. Bd. II. S. 715. Leipzig 1890. — In Wallis: De algebra tractatus. Oxonii 1693 (lateinisch). Cap. XCVIII am Schlusse. S. 422 heisst Frenicles Buch: Solutio duorum problematum circa numeros cubos et quadratos, quae tanquam insolubilia universae Europae mathematicis a clarissimo viro D. Fermat sunt proposita. Hier auch weitere Kritik Wallis über dasselbe. Das Buch ist bis jetzt noch nicht wieder gefunden (G. Eneström, Bibl. Math. 1898. p. 120).

3) Fermat, oeuvres. Tome III. p. 554 (vergl. p. 34).

4) Commerc. epist. No. 19. Fermat, Tome III. p. 496. — Dasselbe No. XXII. Fermat, Tome III. p. 554, siehe auch Anm. 2.

5) Vergl. oben S. 31.

$t^2 - Du^2 = 1$ sogar noch mehr zu leisten, als Fermat eigentlich verlangt habe. Es ist dies bei der klaren und deutlichen Fassung des Problems durch Fermat kaum zu begreifen. Da die ganze Korrespondenz durch Digby [1]) ging, so vermutet Wertheim, der Schreiber Digbys, der die für Brouncker bestimmte Abschrift anfertigte, habe vielleicht die Einleitung der Aufgabe für unerheblich gehalten und deshalb fortgelassen.

Die Briefe, welche im Verlauf der hieran anknüpfenden Auseinandersetzung zwischen Fermat und Frenicle einerseits und Wallis, Brouncker und Schooten andererseits durch die Vermittlung Digbys gewechselt wurden, gab Wallis 1658 unter dem Titel eines „commercium epistolicum" heraus.[2])

Da die Anordnung der Briefe unchronologisch und unübersichtlich ist, füge ich ein Verzeichnis derjenigen bei, welche auf unser Problem Bezug haben, in der Ordnung, wie sie sich inhaltlich aneinander fügen:

Comm. ep. Nr. 8, Februar 1657. (Fermat, Bd. II.) Défi de Fermat (vergl. Seite 31).

Comm. ep. Nr. 9 (Fermat Oeuvres, Bd. III, p. 417). Auszug aus 2 verlorenen Briefen Brounckers an Fermat. Enthält eine Regel zur Auflösung der Gleichung $t^2 - Du^2 = 1$ in Brüchen.[3])

Man nehme $q = \beta^2$ (q, β = num. integ.), $d = q - D$, alsdann ist

$$D\frac{4q}{d^2} + 1 = \left(\frac{q+D}{q-D}\right)^2 \text{ resp.}$$

$$D\left(\frac{4q}{q-D}\right)^2 + 1 = \left(\frac{q+D}{q-D}\right)^2 \text{ oder}$$

$$D\left(\frac{2\beta}{D-\beta^2}\right)^2 + 1 = \left(\frac{D+\beta^2}{D-\beta^2}\right)^2.$$

Das ist genau die gleiche Regel, welche wir (Seite 19ff.) bei den Indern schon gefunden haben.

---

1) Kenelm Digby (1603—1665) lebte zu London, war der Sohn des wegen der Teilnahme an der Pulververschwörung hingerichteten Sir Everard Digby, politisch stark engagiert und befand sich deshalb häufig im Auslande. Wertheim, l. c. S. 557 und 563.

2) Commercium epistolicum edidit John Wallis. Oxford 1658, ferner in Wallis, opera omnia. Bd. II. Oxford 1693, ferner als Anhang in Wallis, de algebra tractatus. Oxford 1685 englisch, 1693 lateinisch, endlich neugedruckt und zum Teil ins Französische übersetzt in Fermat, Oeuvres ed. P. Tannery. Tome III. Paris 1896. p. 399 u. f.

3) Man vergl. Wertheim, l. c. S. 564.

Comm. ep. Nr. 11 (6. Juni 1657). Fermat an Digby. (Fermat Oeuvres, Bd. II, p. 341.) Fermat hat den englisch geschriebenen Brief nicht ordentlich verstehen können; verwirft die „Lösung" von Wallis.

Comm. ep. Nr. 12 (15. August 1657). Fermat an Digby. (Fermat Oeuvres, Bd. II, p. 342.) Fermat bekräftigt im Besitz einer besseren Übersetzung sein Urteil.

Die beiden vorigen Briefe kreuzen sich mit:

Comm. ep. Nr. 20 (27. Sept. 1657). Wallis an Digby. Wallis giebt weitere Regeln zur Lösung der Aufgabe in Brüchen, z. B. diese: D gegeben; man nehme a beliebig $q = \beta^2$; $m = \frac{q}{a}$; p beliebig, $d = \frac{ma}{4p} - pD$, dann ist, wie die Rechnung zeigt,

$$D\left(\frac{\beta}{a}\right)^2 + 1 = D\,\frac{ma}{d^2} + 1 = \left(\frac{\frac{ma}{4p} + pD}{\frac{ma}{4p} - pD}\right)^2.$$

Comm. ep. Nr. 10 (3. Oct. 1657). Brouncker an Wallis. Brouncker hat Nr. 11 und Nr. 12 erhalten und nun endlich die Aufgabe verstanden.

Comm. ep. Nr. 14 (22. Oct. 1657). Brouncker an Wallis. Erster Versuch, ganzzahlige Lösungen zu finden. Resultat: eine Regel, aus einer Lösung neue abzuleiten.

Comm. ep. Nr. 15 (21. Nov. 1657). Wallis an Brouncker. Bespricht die Redaktion des an Fermat abzusendenden Briefes „Placuit reticere methodos quadratum primum .... per inductionem exhibendi.[1])

Comm. ep. Nr. 16 (21. Nov. 1657). Wallis an Digby. Polemisches gegen Fermat; Wallis zeigt, dass die in Nr. 9 gegebene Formel stets alle etwa vorhandenen, ganzen oder gebrochenen Werte liefere, welche die Gleichung $t^2 - Du^2 = 1$ befriedigen; er lobt diese Eigenschaft seiner Lösung und nimmt unberechtigter Weise als selbstverständlich an, unter den Werten $\frac{2\beta}{D - \beta^2}$ müssten sich stets auch ganzzahlige befinden.[1])

Comm. ep. Nr. 17 (7. Dec. 1657). Wallis an Brouncker. Giebt eine Menge Regeln zur Erleichterung des Aufsuchens ganzzahliger Lö-

1) Hierzu Wertheim, l. c. S. 566 unten.

sungen; ausserdem drei Vorschriften, aus einer gegebenen Lösung, vor allem der kleinsten, neue herzuleiten.[1])

Anhang: Auseinandersetzung einer systematischen, für jedes D brauchbaren Methode, deren Form Wallis sich zuschreibt, während der Gedanke von Brouncker herrühren soll.

Comm. ep. Nr. 18 (16. Dec. 1657). Wallis an Digby. Polemik gegen Fermat und besonders gegen Frenicles lateinisches Schriftchen, in welchem Wallis angegriffen wurde. Brouncker wird das Hauptverdienst an der Lösung beigemessen.

Comm. ep. Nr. 19 (20. Jan. 1658). Wallis an Brouncker. Genauere Ausführung der in der Nachschrift zu Nr. 17 dargelegten Methode; Abkürzungen des Verfahrens; Periodizität desselben; Berechnung einiger schwieriger Beispiele, z. B. $D = 433$. Glückwünsche für Brouncker.

Comm. ep. Nr. 26 (20. Febr. 1658). Frenicle an Digby. Frenicle kennt die Briefe Nr. 19 und Nr. 17 noch nicht; er kritisiert die älteren Briefe Wallis. Die Aufgabe sei, eine ganzzahlige Lösung zu finden; man solle an $D = 313$ zeigen, was man könne.

Comm. ep. Nr. 27 (13. März 1658). Brouncker an Digby. Antwort auf das vorige Schreiben. Lösung der Gleichung $t^2 - 313\, u^2 = 1$.

Comm. ep. Nr. 37 (7. April 1658). Fermat an Digby (Oeuvres, Bd. II, p. 374). Fermat kennt erst die Briefe bis zum 21. Nov. 1657, sein Problem sei über die bis dahin gegebenen „petites règles de trivio" erhaben.

Comm. ep. Nr. 32 (13. April 1658). Kritik der Schrift und der Methode Frenicles durch Wallis.

Comm. ep. Nr. 38 (ohne Datum, wahrscheinlich Anfang Mai 1658). Frenicle an Wallis. Frenicle erkennt Wallis neue Lösungsmethode (XVII und IXX) an.

Comm. ep. Nr. 43 (18. Mai 1658). Frenicle an Wallis. Frenicle hat über die neue Lösungsmethode Wallis nunmehr genauere Nachricht und steigert seine Anerkennung zu überschwenglichen und schwülstigen Lobeserhebungen.

Comm. ep. Nr. 45 (am 19. Juni 1658 von Digby nach England abgeschickt). Fermat an Wallis. Fermat erkennt gleichfalls das neue Verfahren an: „Ill. viros etc. quaestionum numericarum a me propositarum solutiones tandem dedisse legitimas libens agnosco imo et gaudeo .... fatentur Galli propositis quaestionibus satisfecisse Anglos."[2])

1) Vergl. Wertheim, l. c. S. 565.

2) Es ist wohl kaum möglich diese Anerkennung Fermats auf etwas anderes

Zu dem „commercium" giebt es noch eine sehr seltene, zuerst von Henry veröffentlichte[1]) anonyme Antwort, welche von Henry Fermat, von Tannery[2]) Frenicle zugeschrieben wird.

Der Verfasser dieser anonymen Replik beklagt die Veröffentlichung der Briefe. Das Buch von „F" (vermutlich Frenicle) habe Wallis die Arbeit vorgethan, da er aus jenem leicht den Kanon habe herausfinden können. „Theorema praecipuum erat: Dato quovis numero etc. . . . . Huius theorematis demonstrationem facilem sibi autor commercii asserit p. 82 et 83 (d. i. ep. 16, siehe Seite 37) imo hanc ibi contineri deserte innuit, sed analystae nostri ne vestigium quidem demonstrationis ilic agnoscunt."

Die Stelle ist merkwürdig. Entweder verlangt „F" den Beweis, dass die Gleichung $t^2 - Du^2 = 1$ stets ganzzahlig lösbar sei; dann hat er Recht. Man begreift aber nicht, wie er nun auf einmal — Fermat oder Frenicle — von seiner früheren Anerkennung zurückgekommen ist. Oder „F" ist mit der Methode des Lösens nicht zufrieden; dann kommt zu der genannten Schwierigkeit noch die hinzu, dass „F" nun die Briefe Nr. 17 und Nr. 19 übersieht.

Es ist der gleiche Widerspruch, welcher, wie früher erwähnt, zwischen den Urteilen besteht, welche Fermat im ep. 45 des comm. ep. und im Brief an Carcavi über die Leistungen Wallis fällt.

Mir scheint die Frage nach der Ursache dieser Ungereimtheit noch offen.

Ich gehe zur Darstellung des von Wallis in den Briefen Nr. 17 und Nr. 19 und im Kap. 98 seiner Algebra angegebenen und Brouncker zugeschriebenen Verfahrens[3]) über. Bei Wallis ist es nicht im allgemeinen, sondern nur an speziellen Beispielen auseinandergesetzt. Der Gedankengang ist etwa folgender:

Vorausgesetzt wird, dass es eine Lösung giebt. Sie werde T, U genannt. Dann ist

$$\text{(I)} \qquad T^2 - DU^2 = 1.$$

Es gilt T und U zu bestimmen. Ist ϱ die nächst kleinere ganze Zahl zu $\sqrt{D}$, so folgt aus der Voraussetzung

---

als das Brounckersche Lösungsverfahren zu beziehen, z. B. auf die Lösung einzelner bestimmter gelöster Aufgaben.

1) Siehe S. 29. Anm. 2.

2) P. Tannery, Fermat, oeuvres. Tome III. Paris 1896. p. 603.

3) Hierzu auch H. Smith, Report on the Theory of numbers. Rep. of the British Assoc. for 1859, Papers I. Oxford 1894. p. 193.

$$\varrho U < T < (\varrho + 1) U,$$

also

$$T = \varrho U + v_1,$$

wo $v_1 < U$ und ganzzahlig. Substituiert man $\varrho U + v_1$ statt T in Gleichung (I), so erhält man

(II) $$Q(U, v_1) = 1$$

ebenfalls in ganzen Zahlen, wenn Q eine homogene quadratische Form bedeutet. Die Gleichung II liefert nun

$$\varrho_1 v_1 < U < (\varrho_1 + 1) v_1,$$
$$U = \varrho_1 v_1 + v_2; \quad v_2 < v_1,$$

(III) $$Q_1(v_1, v_2) = 1$$

und so fort. Da aber vorausgesetzt ist, es gebe eine ganzzahlige Lösung der Gleichung $t^2 - Du^2 = 1$, und da die Zahlen T, U, etc. eine abnehmende Reihe bilden,

$$T > U > v_1 > v_2 \text{ etc.},$$

so muss einmal eine Gleichung

$$Q_n(v_n, v_{n+1}) = 1$$

erreicht werden, welche

$$v_n = \varrho_n v_{n+1}$$

und somit vermöge der gemachten Voraussetzung über die Lösbarkeit von $t^2 - Du^2 = 1$ auch einen ganzzahligen Wert für v_{n+1} liefert.

Durch Einsetzen des gefundenen v_{n+1} erhält man nun, ähnlich wie bei dem Algorithmus zur Bestimmung des grössten gemeinschaftlichen Teilers zweier Zahlen die Werte T und U.

Man sieht, dass das angegebene Verfahren stets zum Ziele führen muss, sofern nur feststeht, dass es eine Lösung T, U giebt und, sofern es gelingt, aus den Gleichungen $Q_k = 1$ die Ungleichungen resp. Substitutionen für die v_k zu ermitteln.

Beispiel

(I) $$T^2 - 13 U^2 = 1,$$
$$\varrho = 3,$$
$$3U < T < 4U; \quad T = 3U + v_1.$$

(II) $$Q(U, v_1) = -4U^2 + 6Uv_1 + v_1^2 = 1,$$
$$\varrho_1 = 1,$$
$$v_1 < U < 2v_1; \quad U = v_1 + v_2.$$

(III) $$Q(v_1, v_2) = 3v_1^2 - 2v_1 v_2 - 4v_2^2 = 1,$$
$$\rho_2 = 1,$$
$$v_2 < v_1 < 2v_2;\quad v_1 = v_2 + v_3.$$

(IV) $$Q(v_2, v_3) = 3v_2^2 + 4v_2 v_3 + 3v_3^2 = 1,$$
$$\rho_3 = 1,$$
$$v_3 < v_2 < 2v_3;\quad v_2 = v_3 + v_4.$$

(V) $$Q(v_3, v_4) = 4v_3^2 - 2v_3 v_4 - 3v_4^2 = 1,$$
$$\rho_4 = 1,$$
$$v_4 < v_3 < 2v_4;\quad v_3 = v_4 + v_5.$$

(VI) $$Q(v_4, v_5) = -v_4^2 - 6v_4 v_5 + 4v_5^2 = 1,$$
$$\rho_5 = 6,$$
$$6v_5 < v_4 < 7v_5;\quad v_4 = 6v_5 + v_6.$$

(VII) $$Q(v_5, v_6) = 4v_5^2 - 6v_5 v_6 - v_6^2 = 1,$$
$$\rho_6 = 1,$$
$$v_6 < v_5 < 2v_6;\quad v_5 = v_6 + v_7.$$

(VIII) $$Q(v_6, v_7) = -3v_6^2 + 2v_6 v_7 + 4v_7^2 = 1,$$
$$\rho_7 = 1,$$
$$v_7 < v_6 < 2v_7;\quad v_6 = v_7 + v_8.$$

(IX) $$Q(v_7, v_8) = 3v_7^2 - 4v_7 v_8 - 3v_8^2 = 1,$$
$$\rho_8 = 1,$$
$$v_8 < v_7 < 2v_8;\quad v_7 = v_8 + v_9.$$

(X) $$Q(v_8, v_9) = -4v_8^2 + 2v_8 v_9 + 3v_9^2 = 1,$$
$$\rho_9 = 1,$$
$$v_9 < v_8 < 2v_9;\quad v_8 = v_9 + v_{10}.$$

(XI) $$Q(v_9, v_{10}) = v_9^2 - 6v_9 v_{10} - 4v_{10}^2 = 1,$$
hieraus
$$v_9 = 1,\quad v_{10} = 0$$
und so
$$T = 649;\quad U = 180.$$

Es fällt sogleich auf, dass die Formenkette der Q mit der einen zu $D = 13$ gehörigen Periode identisch ist; ebenso, dass vermöge der an-

gewandten Substitutionen für T, U und v, $\frac{T}{U}$ in einen Kettenbruch verwandelt wird.[1]) Denn man erhält

$$\frac{T}{U} = 3 + \frac{v_1}{U} = 3 + \frac{v_1}{v_1 + v_2}$$

$$= 3 + \cfrac{1}{1 + \cfrac{v_2}{v_1}} = 3 + \cfrac{1}{1 + \cfrac{v_2}{v_2 + v_3}} = 3 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{v_3}{v_2}}}$$

u. s. w. bis

$$\frac{T}{U} = 3 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{6 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1}}}}}}}}} \text{ etc.}$$

der ersten Doppel-Periode in der Kettenbruchentwicklung von $\sqrt{13}$.

Würde man nicht, wie wir, in $Q(v_9, v_{10})$; $v_9 = 1$, $v_{10} = 0$ gesetzt haben, sondern in der ursprünglichen Weise fortgefahren sein, so hätte man bekommen

$$\varrho_{10} = 6,$$

$$6v_{10} < v_9 < 7v_{10}; \quad v_9 = 6v_{10} + v_{11},$$

$$Q(v_{10}, v_{11}) = -4v_{10} + 6v_{10}v_{11} + v_{11}^2 = 1.$$

Da diese Form aber mit $Q(U, v_1)$ identisch ist, würde sich die gesamte Rechnung wiederholt haben, und man hätte bei Q_{20} oder weiterhin Q_{30}, Q_{40} etc. die Möglichkeit gehabt, neue Lösungen zu erhalten. Diese Periodizität wurde von Wallis wohl bemerkt, ebenso wie der Umstand, dass man alle Lösungen bekommt, wenn man ein, zwei u. s. w. Perioden weit geht; doch scheint er keinen Versuch gemacht zu haben, die Notwendigkeit dieser Eigenschaften zu beweisen.

Dieselbe erhellt übrigens leicht aus dem Zusammenhang des Ver-

1) H. Smith, Report on the theorie of numbers. Rep. of the British Assoc. for 1859; Coll. Papers. I. p. 193. Oxford 1894.

fahrens, entweder mit der Entwicklung von $\sqrt{D}$ in einen Kettenbruch oder mit den Perioden der zugehörigen reduzierten quadratischen Formen.[1])

Ausser der allgemeinen Methode giebt Wallis noch eine Anzahl Regeln, um aus einer Lösung neue herzuleiten und um die Rechnung abzukürzen. Ich erwähne von diesen nur die Benutzung negativer v_k, in den oben angegebenen Substitutionen. Dies Verfahren, das auf die Entwicklung einer Quadratwurzel in einen Kettenbruch mit teils positiven, teils negativen Teilnennern hinauslaufen würde, führt in der That manchmal rascher zum Ziel. Doch ist es nicht, wie Wallis meint, in allen Fällen richtig. Lagrange zeigt dies in seinen „Additions“ etc.[2]) an einem Beispiel. Ich werde später noch darauf einzugehen haben.[3])

Es ist schon hervorgehoben worden, dass die Methode von Wallis sich auf den Satz stützt, dass die Gleichung $t^2 - Du^2 = 1$ stets ganzzahlig befriedigt werden kann. Den Beweis dafür, den schon Fermat verlangt hatte, sucht Wallis in seiner Algebra[4]) zu erbringen. Er stützt sich hierbei auf folgendes Lemma:

„Es sei m die nächst grössere ganze Zahl zu dem irrationalen Werte $\sqrt{D}$, so dass $m - \sqrt{D} < 1$; man setze $p = m - \sqrt{D}$; $r = \frac{1}{2\sqrt{D}}$; dann ist es möglich, zwei ganze Zahlen z und a so zu wählen, dass

$$\frac{z}{a} < p < \frac{\sqrt{z^2 + 4pr} + z}{2a}.$$

Nimmt man dieses Lemma als bewiesen an, so würde in der That folgen, dass $t^2 - Du^2 = 1$ ganzzahlig lösbar sei. Denn da

$$\frac{z}{a} < p, \text{ ist } ap - z > 0,$$

und da

$$p < \frac{\sqrt{z^2 + 4pr} + z}{2a},$$

1) Lagrange hat das Wallissche Verfahren direkt aus der Auflösung der Gleichung $t^2 - Du^2 = 1$ vermittelst der Näherungsbrüche des Kettenbruches für $\sqrt{D}$ abgeleitet in „Additions aux élémens d'Euler“. § VIII. Oeuvres Tome 7ième. Paris 1877. p. 160.

2) Siehe Anm. 1, l. c. p. 162.

3) Minnigerode, Göttingische gelehrte Anzeigen 1873. Bd. III. p. 619. Über eine neue Methode, die Pellsche Gleichung aufzulösen.

4) Wallis, de algebra tractatus. Oxford 1693. Cap. XCIX. p. 427 u. 428.

wird

$$2ap - z < \sqrt{z^2 + 4pr},$$

$$4a^2p^2 - 4apz + z^2 < z^2 + 4pr,$$

$$ap - z < \frac{r}{a} = \frac{1}{2a\sqrt{D}},$$

$$am - a\sqrt{D} - z < \frac{1}{2a\sqrt{D}},$$

also

$$am - z < a\sqrt{D} + \frac{1}{2a\sqrt{D}}.$$

$am - z$ ist eine ganze Zahl, sie heisse l. Dann ist

$$l^2 < (a^2D + 1) + \frac{1}{4a^2D};$$

da ferner, wie bewiesen

$$ap - z > 0$$

oder

$$am - a\sqrt{D} - z > 0,$$

wird

$$am - z \text{ oder } l > a\sqrt{D},$$

somit

$$l^2 > a^2D,$$

also

$$a^2D < l^2 < (a^2D + 1) + \frac{1}{4a^2D}.$$

Da nun $a^2D + 1$ die einzige zwischen diesen beiden Grenzen liegende ganze Zahl ist, muss $l^2 = a^2D + 1$ sein, d. h. die Gleichung $t^2 - Du^2 = 1$ wird durch die Zahlen l und a befriedigt, ist also ganzzahlig lösbar.

Es würde somit nur das Lemma zu beweisen sein. Wallis macht folgendermassen einen Versuch.[1])

Man bestimme zunächst $\frac{z}{a} < p$, das gehe immer: „sed eo tam prope

1) Wallis, l. c. p. 428.

accedat ut defectus sit dato (: hier schleicht sich der Fehler ein) minor".
Dann setzt man $p - \frac{z}{a} = y$, so dass

$$p = \frac{z}{a} + y < \frac{\sqrt{z^2 + 4pr} + z}{2a}.$$

Ferner setzt man

$$\frac{\sqrt{z^2 + 4pr} + z}{2a} = p + x$$

und

$$y + x = \frac{v}{a}.$$

$$\frac{z + v}{a} = \frac{\sqrt{z^2 + 4pr} + z}{2a},$$

$$v = \frac{\sqrt{z^2 + 4pr} - z}{2}.$$

„Quod omnio est possibile", d. h. also man könne nun z so wählen, dass diese Gleichung erfüllt sei „adeoque lemma bene assumptum".

Gauss und Lagrange[1]) haben schon hervorgehoben, dass dieser Schluss von Wallis falsch ist. Gauss sagt[2]):

„Quae Wallisius ad hunc finem (sc. demonstrationem, a inveniri posse) protulit, nihil ponderis habent. Paralogismus in eo consistit, quod p. 428 supponit proposita quantitate p inveniri posse numeros integros a, z tales ut $\frac{z}{a}$ minor sit quam p defectus vero assignato minor. Hoc utique verum est quando defectus assignatus est quantitas data, neque vero, quando ab a et z pendet, adeoque variabilis est, ut in casu prae-

1) Lagrange, Solution d'un problème d'Arithmétique (1779). Oeuvres Tome I. Paris 1867. p. 672. „..il est vrai que Monsieur Wallis a prétendu la prouver, mais par un raisonnement que les mathématiciens trouveront bien peu satisfaisant et qui n'est ce me semble dans le fond q'une espèce de pétition de principe." — Ders., Additions aux élémens d'Euler. § VIII. Oeuvres Tome VII. p. 158. Paris 1877. „Wallis, il est vrai, a prétendu la première de ces propositions (den Möglichkeitsbeweis) mais sa démonstration n'est, j'ose le dire, qu'une simple pétition de principe." Es scheint mir nicht ohne Interesse, die beiden Kritiken von Gauss und Lagrange zu vergleichen.

2) Gauss, Disq. Arithm. Art. 202. Werke I. S. 196.

cedenti evenit." Denn da $x + y = \frac{z}{a}\left(\frac{\sqrt{1+\frac{4pr}{z^2}}-1}{2}\right)$, pr konstant, $\frac{z}{a} < p$, $v = z\left(\frac{\sqrt{1+\frac{4pr}{z^2}}-1}{2}\right)$, nähern sich v und $p - \frac{z}{a}$ gleichzeitig der 0.

Mit dem Lemma fällt aber der ganze Beweis Wallis.

Indes wird dadurch die Brauchbarkeit des eigentlichen Auflösungsverfahrens nicht beeinträchtigt, da man es ja mit Lagrange[1]) aus anderen Verfahren ableiten oder den fehlenden Existenzbeweis etwa in der von Dirichlet angegebenen Weise[2]) ergänzen kann.

Die Methode von Wallis und Brouncker ist von verschiedenen Mathematikern verschieden beurteilt worden.

Der Äusserungen Fermats und Frenicles ist bereits früher gedacht worden. Huyghens vermisste einen Beweis dafür, dass die Methode stets zum Ziele führe.[3])

Euler druckte die Wallis-Brounckersche Lösung fast wörtlich im Cap. VII Art. 98 seiner Algebra ab[4]) und bemerkt:

„.... hat ein gelehrter Engländer, Namens Pell eine sehr sinnreiche Methode erfunden, welche wir hier erklären wollen. Dieselbe ist aber nicht so beschaffen, dass sie auf allgemeine Art für jede Zahl a, sondern nur für jeden besonderen Fall gebraucht werden kann".

Ein anderes Mal heisst es[5]):

„.... a solutionis ingeniosissimae auctore Pellianum vocatum" oder „.... etiamsi autem solutio Pelliana huius problematis sit elegantissima."

Lagrange, so scheint es, änderte im Laufe der Zeit seine Ansicht. 1768 schreibt er an d'Alembert[6]):

„.... nous n'avons que je sache que la solution de Wallis qui est

1) Lagrange, Addition, aux élémens d'algèbre d'Euler (1774). Oeuvres. Bd. VII. p. 158. § VIII.

2) Dirichlet, Vorlesungen über Zahlentheorie herausg. v. Dedekind. 4. Aufl. Braunschweig 1894. Nr. VIII. S. 371.

3) Huyghens, Oeuvres II. p. 211.

4) Hierzu auch Anm. 1, S. 33.

5) Euler, Opera arithmetica vom Jahre 1759. Nov, comm. Petrop. XI. 1765. Oct. 15. Opera minora coll. Nr. XXIII. p. 317.

6) Lagrange, Brief an d'Alembert vom 15. Aug. 1768. Oeuvres. Bd. XIII. Paris 1890. p. 118.

d'ailleurs fort imparfaite et qui ne consiste, que dans une espèce de tâtonnement . ." und entsprechend in „Solution d'un problème etc." „mais la méthode de ce savant géomètre (Wallis) ne consiste, que dans une espèce de tâtonnement, par lequel on n'arrive au but que d'une manière assez incertaine et sans savoir même, si l'on arrivera".[1]) Später nennt er die Lösung „ingénieuse"[2]) und zeigt, dass sie der Sache nach mit der Kettenbruchmethode identisch ist.[3])

Des genauen und gerechten Urteils von Gauss haben wir schon gedacht; er fügt hinzu:[4])

„Omnes hae solutiones, si essentiam spectas, conveniunt cum ea, quam obtinemus, ei in art. 198 formam reductam eam adoptamus, in qua $a = 1$."

Seitdem hat es der Methode nicht an gerechter Würdigung gefehlt, wie die Urteile Legendres[5]), Dirichlets[6]) und anderer zeigen.

Es muss daher verwundern, dass man in neueren Lehrbüchern, wie z. B. selbst bei Bachmann[7]) Aussprüchen begegnet, wie diesem:

„. . . . waren die Methoden nicht geeignet, dieselbe (sc. Lösung) mit Notwendigkeit, ihre Existenz einmal angenommen, finden zu lassen.

§ 3. Euler.

Auf die Leistung von Wallis und Brouncker folgten, so scheint es, fast 100 für die Theorie unserer Gleichung unfruchtbare Jahre.

Allerdings hörte man in Frankreich nicht auf, sich mit dem Fermatschen Problem zu beschäftigen. Claude Jaquemet[8]) ver-

---

1) Lagrange, Oeuvres. Bd. I. Paris (1867). p. 672.

2) Lagrange, „Additions". § VIII. Oeuvres VII. p. 158 l. 9 von unten.

3) Lagrange, l. c. p. 159 u. f.

4) Gauss, Disquis. Arithmeticae, Art. 202. Werke I. p. 196.

5) Legendre, A. M., Théorie des nombres. IIIième édition. Paris 1810. p. 58.

6) Dirichlet-Dedekind, Vorlesungen über Zahlentheorie. 4. Auflage. Braunschweig 1894. p. 200. — Ders., Einige Sätze über unbestimmte Gleichungen. (1834). Ges. Werke. Berlin 1889. Bd. I. p. 222.

7) Bachmann, Elemente der Zahlentheorie. 2. Bd. 8⁰. Leipzig 1892. Bd. I. S. 189.

8) Handschriftliches Fragment Jaquemets (1651—1729) veröffentlicht in: Recherches sur les manuscrits de Fermat suivies de Fragments inédits de Bachet et de Malebranche par C. Henry, Bulletino di Bibliografia e di storia delle scienze matematiche et fisiche. Pubblicato da B. Boncampagni. Tomo XII. Roma 1879. p. 696. Nr. XIII und von diesem Malebranche zugeschrieben, es kommt jedoch Jaquemet zu, vergl. Deux mathematiciens de l'oratoire par Aristide Marre. l. c. (Bull. etc.) p. 886 und Cantor, Vorles. über Geschichte der Mathematik. Bd. III. 1. Abteil. Leipzig 1894. S. 98.

suchte sich ohne Kenntnis des Inhaltes der Wallisschen Schriften daran, kam aber nur bis zu einer ganz elementaren Regel, aus einer Lösung der Gleichung eine neue abzuleiten. Ozanam reproduzierte, wie bereits besprochen, in seiner Algebra die Wallis-Brounckersche Lösung.[1][2])

Jedoch scheint Euler der erste gewesen zu sein, der wieder selbständig die Theorie der ganzzahligen Auflösung der Gleichung $t^2 - Du^2 = 1$ zu fördern suchte. Der Anlass für ihn war die Reduktion der unbestimmten binären quadratischen Gleichung. In einem Briefe an Goldbach vom 10. Aug. 1730 erwähnt er[3]), er brauche die Auflösung der Gleichung $t^2 - Du^2 = 1$, um $ax^2 + bx + c$ zu einem vollen Quadrat zu machen, und fügt hinzu:

„Agitata sunt huiusmodi problemata in numeris integris inter Wallisium et Fermatium .... exemplum maxime difficile erat, invenire numeros integros qui loco x positi $109x^2 + 1$ efficiant quadratum .... Pro huiusmodi quaestionibus solvendis excogitavit D. Pell Anglus peculiarem methodum in Wallisii operibus expositam .... exque ad institutum meum opus habeo ut $1 + a\lambda^2$ fiat quadratum. — Ea vero methodus tantum ad exempla prorsus numerica patet, neque eius est usus in formulis arbitrarios coefficientes habentibus resolvendis“.

Euler schreibt also bereits hier die Wallis-Brounckersche Methode Pell zu. Schon bei früherer Gelegenheit[4]) wurde erwähnt, dass er zu diesem Irrtum durch die englische Übersetzung der Algebra Rahns gekommen sein soll. Mir scheint, dass diese Annahme nicht zu dem Inhalte des citierten Briefes passt. Denn Euler spricht in diesem

---

1) v. Anm. 7, S. 32.

2) Es lag nahe, bei Michel Rolle (1652—1719), vielleicht dem bedeutendsten französischen Zahlentheoretiker der damaligen Zeit, der sich viel mit unbestimmten Gleichungen befasst hat, nach einer Beschäftigung mit unserem Problem zu suchen. In seiner „Algebra“ (Traité d'algèbre 1690 Paris, vergl. auch Cantor. Bd. III. 1. Abteil. p. 98) findet sich indes nichts darüber, und auch das Buch: Méthodes pour résoudres les questions indéterminées de l'algèbre par M. Rolle. A Paris chez Jean Cusson 1699, scheint nichts darüber zu enthalten. Ein Exemplar dieser seltenen Schrift befindet sich, wie mir Herr Hofr. Prof. Dr. Cantor so gütig war, mitzuteilen, in der Münchener Hof- und Staatsbibliothek. Ich war in der That so glücklich, es daher zu erhalten. Leider ist es jedoch fast ganz in Worten geschrieben und sehr dunkel und schwerverständlich, namentlich wegen der fortwährenden Beziehungen auf andere Schriften des gleichen Verfassers, so dass ein sicheres Urteil, ob der Verfasser das in Rede stehende Thema berührt hat, kaum zu gewinnen ist. Unter den Beispielen befindet sich keine Gleichung der Form $t^2 - Du^2 = 1$.

3) Correspondance mathématique et physique de quelques célèbres géomètres du XVIIIième siècle publiée par P. H. Fuss. Pétersbourg 1843. Bd. I. p. 37.

4) v. Anm. 1, S. 33.

ausdrücklich davon[1]), dass das Problem zwischen Wallis und Fermat verhandelt worden sei, und weiss, dass die Lösungsmethode in Wallis Werken steht. Es scheint mir nicht unmöglich, dass die Überschrift des betreffenden Abschnittes der Algebra von Wallis, die in der That leicht zu Missverständnissen führen kann, an dem Versehen Eulers schuld ist, zumal da er die Auseinandersetzung bei Wallis oder Brouncker nur flüchtig gelesen hat; sonst müsste er wissen, dass nicht $D = 109$, sondern $D = 433$ oder $D = 313$ die schwierigsten der gelösten Beispiele waren. Auch bemerkt man, wie Euler im Lauf der Jahre immer bestimmter von „Pell" spricht. Während er 1732[2]) und selbst noch 1755[3]) Pell und Fermat als gleichberechtigt nennt, ist 1773[4]) Pell allein übrig geblieben.

Das Ergebnis der Beschäftigung mit dem Problem, von welcher der Brief an Goldbach erzählt, finden wir niedergelegt in der Abhandlung „De solutione problematum Diophanteorum per numeros integros".[1]) Sie enthält die Bemerkung, die Euler später dazu führte, die Gleichung $t^2 - Du^2 = 1$ mit Hilfe eines Kettenbruchalgorithmus aufzulösen. Nachdem gezeigt worden ist, dass man aus einer gegebenen Lösung p, q eine neue mittelst der Formel $q_1 = 2q^2 - 1$, $p_1 = pq - 0$, allgemein $q_n = 2qq_{n-1} - q_{n-2}$, $p_n = qp_{n-1} - p_{n-2}$ ableiten könne, giebt Euler für eine Anzahl spezieller Werte von D allgemeine Lösungsformeln

$$D = e^2 - 1; \quad t = e; \quad u = 1$$

$$D = e^2 + 1; \quad t = 2e^2 + 1; \quad u = 2e \text{ etc.}$$

$$D = \alpha^2 e^{2b} \pm 2\alpha e^{b-1}; \quad t = \alpha e^{b-1} \pm 1; \quad u = e$$

$$D = (\alpha e^b + \beta e^m)^2 + 2\alpha e^{b-1} + 2\beta e^{m-1}; \quad t = \alpha e^{b-1} + \beta e^{m+1} + 1; \quad u = e$$

$$D = \frac{1}{4}\alpha^2 R^2 e^{2b} \pm \alpha e^{b-1}; \quad t = \frac{1}{2}\alpha R^2 e^{b+1} \pm 1; \quad u = Re.$$

1) Ebenso in: De solutione problematum Diophanteorum per numeros integros. Comment. VI. 1732. p. 175. § 15. L. Euleri opera minora collecta. Tomus I. l. c. — Ders., Commentationes arithmeticae collectae Tomus prior. ed. N. Fuss et P. H. Fuss. Petropoli 1849. p. 7.

2) l. c. p. 7.

3) Euler an Goldbach. 23. Aug. 1755. Correspondance etc. S. 629. vergl. S. 48.

4) Euler, nova subsidia pro resolutione formulae $ax^2 + 1 = y^2$. Opusc. analyt. I. p. 310. Comm. arithmeticae collectae ed. N. Fuss. Petropoli 1849. Tomus posterior. p. 35.

Ist D nicht in einer dieser Formeln enthalten, so wird die kleinste Auflösung T, U vermittelst des Verfahrens von Wallis ermittelt. In § 18 bemerkt Euler dann: „Hic statim occurrit modus perfacilis extrahendi quam proxime radicem quadratam ex numero quocunque non quadrato D". Es folge nämlich aus

$$q^2 - Dp^2 = 1, \qquad \sqrt{D} = \frac{\sqrt{q^2 - 1}}{p},$$

„quam proxime" und zwar um so genauer, je grösser q. Kenne man also ein p, q, so könne man daraus immer neue und grössere mit Hilfe der früheren Regel ableiten, somit immer genauere Näherungsbrüche für $\sqrt{D}$ bekommen. Der Fehler sei kleiner als $\frac{1}{2p^2\sqrt{D}}$.

Man sieht, es ist der gleiche Weg, welchen nach Tannerys Ansicht auch Archimed zur Berechnung von $\sqrt{D}$ benutzte, und Euler brauchte ihn nur in umgekehrter Richtung zu gehen; um darauf zu kommen, die Gleichung $t^2 - Du^2 = 1$ vermittelst der Näherungsbrüche der Kettenbruchentwicklung für $\sqrt{D}$ (die ja hier noch ganz aus dem Spiel bleibt) zu lösen.

Doch that er diesen Schritt, scheint es, zunächst noch nicht. Allerdings spricht er 1753 und 1755 — also fast 20 Jahre später — in Briefen an Goldbach [1]) von einer „gewissen" Methode und von Verbesserungen, welche er an der „Pell"schen angebracht habe, er bringt indes in der nächsten Abhandlung, in welcher er auf die Gleichung $t^2 - Du^2 = 1$ eingeht, nichts davon. Ich erwähne aus dem 1762 erschienenen Aufsatze [2]) nur die observatio § 30, auf welche Euler grosses Gewicht legt, nämlich den Satz, dass aus

$$Da^2 + p = b^2, \qquad Da_1{}^2 + p_1 = b_1{}^2$$

folgt

$$D(ab_1 \pm ba_1)^2 + pp_1 = (bb_1 \pm Daa_1)^2$$

folgt. Wir haben gesehen, dass die Inder schon diesen Satz kannten und bewiesen.

---

1) Correspondance etc. (v. p. 48), p. 614 u. f. Euler an Goldbach 4. IX. 1753. ib. p. 629 u. f. — Euler an Goldbach 23. IX. 1755.

2) De resolutione formularum quadraticarum indeterminatarum per numeros integros. Nov. Comm. IX. 1762. p. 3. — Comment. arithm. collect. ed. P. u. N. Fuss. Petropoli 1849. Tomus prior. p. 297.

Drei Jahre nach der genannten Abhandlung, zu einer Zeit, als auch Lagrange schon begonnen hatte, das Problem zu bearbeiten, veröffentlichte Euler den Aufsatz: „De usu novi algorithmi in problemate Pelliano solvendo".[1]) In demselben schlägt er den 1732 nicht benutzten Weg ein, indem er nun umgekehrt wie damals die Berechnung der Näherungsbrüche für $\sqrt{D}$ zur Lösung der Gleichung $t^2 - Du^2 = 1$ benutzt.

Der Aufsatz enthält fast alles, was zu einem strengen Beweise, der Existenz einer Lösung und des notwendigen Erfolges des Verfahrens erforderlich ist, ohne dass Euler, so scheint es, das Bedürfnis nach einem solchen Beweise empfunden hätte und entsprechende Versuche machte.[2])

Euler geht von der Bemerkung aus, dass, wenn

$$q^2 - Dp^2 = 1, \qquad \frac{q}{p}$$

ein Näherungsbruch für $\sqrt{D}$ sei, „quae valorem irrationalem $\sqrt{D}$ tam prope exprimat, seu eum tam parum excedat, ut id nisi maioribus numeris adhibendis accuratius fieri nequeat". Der Beweis hierfür fehlt. Man müsse nun, fährt Euler fort, auf irgend welchem Wege Näherungsbrüche für $\sqrt{D}$ berechnen und die passenden unter ihnen ermitteln.

Hierzu benutzt er die Entwicklung von $\sqrt{D}$ in einen Kettenbruch mit positiven Teilnennern. Er setzt

$$\sqrt{D} = A + \frac{1}{x}, \quad \text{so dass} \quad D - A^2 < 1$$

$$x = \frac{\sqrt{D} + A}{D - A^2};$$

$$D - A^2 = \alpha; \qquad A = v$$

$$x = a + \frac{1}{y},$$

wo a die grösste ganze Zahl in

$$\frac{\sqrt{D} + A}{\alpha} \quad \text{oder} \quad \frac{v + A}{\alpha},$$

1) De usu novi algorithmi in problemate Pelliano solvendo. Nov. Comm. XI. 1765. — Comm. arithm. collectae. ed. P. et N. Fuss. Petropoli 1849. Tomus prior. p. 316.

2) Vergl. Smith, Coll. Papers. Bd. I. S. 192. Oxford 1894.

$$y = \frac{\alpha(\sqrt{D} + a\alpha - A)}{D - A^2 + 2aA\alpha - a^2\alpha^2}$$

$$= \frac{\alpha(\sqrt{D} + a\alpha - A)}{\alpha(1 + a[A - \{a\alpha - A\}])},$$

also wenn

$$a\alpha - A = B; \quad 1 + a(A - B) = \beta$$

so wird

$$y = \frac{\sqrt{D} + B}{\beta} = b + \frac{1}{x},$$

wenn b die grösste ganze Zahl in $\frac{\sqrt{D} + B}{\beta}$ oder $\frac{v + B}{\beta}$.

Indem man so fortfährt, bekommt man das Schema:

$A = v$	$\alpha = D - A^2 = D - v^2$	$a \leq \frac{v + A}{\alpha}$
$B = a\alpha - A$	$\beta = \frac{D - B^2}{\alpha} = 1 + a(A - B)$	$b \leq \frac{v + B}{\beta}$
$C = \beta b - B$	$\gamma = \frac{D - C^2}{\beta} = \alpha + b(B - C)$	$c \leq \frac{v + C}{\gamma}$
$D = \delta c - C$	$\delta = \frac{D - D^2}{\gamma} = \beta + c(C - D_1)$	$d \leq \frac{v + D}{\delta}$ etc.

Aus der Berechnung von $\beta = \frac{D - B^2}{\alpha}$ folgt, ohne dass **Euler** es noch besonders bemerkte, dass in der That

$$\beta = \frac{D - B^2}{\alpha} = 1 + a(A - B)$$

und ebenso wie γ, δ etc. ganzzahlig ist.

Da

$$a < \frac{v + A}{\alpha},$$

sei ferner, so führt **Euler** aus

$$a\alpha \leq v + A \quad \text{also} \quad B \leq v.$$

Im Falle

$$B = v \text{ werde } b = 2v, \quad \beta = 1;$$

weiter da

$$b \leq \frac{v + B}{\beta},$$

$$b\beta = B \leq v, \quad \text{also } C \leq v \text{ etc.}$$

Die Zahlen B, C etc. müssten also sämtlich kleiner oder gleich v sein und dem entsprechend die Grössen β, γ etc. grösser oder gleich 1 die Grössen b, c etc. kleiner oder gleich $2v$; sobald aber dieser letztere Fall eintrete, also $M = v$, $\mu = 1$, $m = 2v$ werde, beginne die Entwicklung von neuem, wie sie angefangen.

Ob indes der Fall $M = v$ wirklich notwendig wiederkehren muss, wird nicht weiter untersucht, an Beispielen die Periodizität der Grössen α, β etc. und a, b, c etc. festgestellt, und es werden für gewisse Formen von D die Werte a, b, c etc. allgemein ermittelt.

Nun gilt es, aus der Kettenbruchentwicklung für $\sqrt{D}$ Näherungsbrüche zu gewinnen und unter ihnen die passenden auszusuchen. Dazu untersucht Euler zunächst die Eigenschaften der Näherungsbrüche eines Kettenbruches. Er giebt das Bildungsgesetz derselben, indem er die Reihen

Teilnenner	$v;\ a;\ b \cdots\cdots\cdots M;\ n$
Näherungsbrüche	$\frac{1}{0};\ \frac{v}{1};\ \frac{av+1}{a} \cdots\cdots \frac{M}{P};\ \frac{N}{Q};\ \frac{nN+M}{nQ+P}$

hinschreibt und führt dann eine abkürzende Bezeichnung ein, nämlich

$$\frac{1}{0};\ \frac{(v)}{1};\ \frac{(v,a)}{(a)};\ \frac{(v,a,b)}{(a,b)} \text{ etc.,}$$

wo

$$(v,a) = (v)a + 1; \quad (v,a,b) = (v,a)b + v \text{ etc.,}$$

$$(a) = 1(a) + 0; \quad (a,b) = b(a) + 1 \text{ etc.}$$

und sagt ohne Beweis „deinde etiam sequentes transformationes demonstravi“

$$(v,a,b,c,d,e) = v(a,b,c,d,e) + (b,c,d,e),$$
$$(v,a,b,c,d,e) = (v,a)(b,c,d,e) + v(c,d,e),$$
$$(v,a,b,c,d,e) = (v,a,b)(c,d,e) + (v,a)(d,e),$$
$$(v,a,b,c,d,e) = (v,a,b,c)(d,e) + (v,a,b)(e).$$

Unter den nach dem angegebenen Algorithmus gewonnenen Näherungsbrüchen für $\sqrt{D}$ müssen jetzt die zur Lösung der Gleichung $t^2 - Du^2 = 1$ brauchbaren herausgefunden werden. Dies gelingt Euler mit Hilfe des Satzes, dass, wenn $\frac{M}{N}$ der $n$te Näherungsbruch, und μ der

zugehörige Index

$$M^2 - DN^2 = (-1)^n \mu$$

(der fingierte Näherungsbruch $\frac{1}{0}$ ist als solcher nicht mitgezählt).

So oft nämlich $\mu = 1$ und gleichzeitig n gerade werde, sei M, N eine Lösung der Gleichung $t^2 - Du^2 = 1$; nun werde aber jedesmal $\mu = 1$, wenn der zugehörige Teilnenner $= 2v$ werde, somit am Schluss jeder Periode des Kettenbruches; ob

$$M^2 - DN^2 = \pm \mu$$

werde, hänge davon ab, ob die Periode eine gerade oder eine ungerade Gliederzahl besitze; im ersteren Falle erhalte man direkt die gesuchte Lösung, im zweiten müsse man zwei Perioden weit gehen oder aus

$$M^2 - DN^2 = -1$$

eine Lösung der Gleichung $t^2 - Du^2 = 1$ ableiten, indem man $t = 2M^2 + 1$, $u = 2MN$ setze.

Der Satz, auf welchen sich diese Überlegung stützt, wird jedoch nicht streng bewiesen, vielmehr begnügt sich Euler, durch Berechnung zu zeigen, dass er für die ersten Näherungsbrüche von $\sqrt{D}$ richtig ist.

Damit ist, abgesehen von dem Nachweis, dass man in der That auf dem angegebenen Wege stets zum Ziele kommen muss, alles beisammen, was zur Ermittlung der kleinsten Lösung der Gleichung $t^2 - Du^2 = 1$ nötig ist.

Doch erleichtert sich Euler noch die Rechnung mit Hilfe des ohne Beweis angegebenen Lehrsatzes, dass

$$\begin{aligned}
&(v, a, b, c, d, e \cdots lm)\\
&= v(ab \cdots lm) + (bc \cdots lm)\\
&= (va)(bc \cdots lm) + v(cd \cdots lm)\\
&= (vab)(c \cdots lm) + (va)(d \cdots lm) \text{ etc.}
\end{aligned}$$

Denn zufolge desselben genügt es, die Näherungsbrüche eine Stelle weiter als bis zur Mitte der ersten Periode des Kettenbruches zu berechnen.

Setzt man mit Euler ferner den Satz

$$(vab \cdots lm) = (ml \cdots av)$$

als bewiesen voraus, so folgt das Behauptete folgendermassen.

I. Fall. Die Periode des Kettenbruches für $\sqrt{D}$ ist von ungerader Gliederzahl. Sie heisse

$$vab \cdots lmml \cdots ba2v$$

und

$$\frac{P_1}{Q_1};\ \frac{P_2}{Q_2} \cdots \frac{P_{\mu-1}}{Q_{\mu-1}};\ \frac{P_\mu}{Q_\mu};\ \frac{P_{\mu+1}}{Q_{\mu+1}} \cdots \frac{P_{2\mu-1}}{Q_{2\mu-1}};\ \frac{P_{2\mu}}{Q_{2\mu}}$$

seien die entsprechenden Näherungsbrüche $\left(\frac{P_1}{Q_1} = \frac{1}{0}\right.$ der fingierte$\left.\right)$. Dann ist

$$(P_{2\mu})^2 - D(Q_{2\mu})^2 = (-1)^{2\mu-1} = -1,$$

also $t^2 - Du^2 = 1$, wenn man $t = 2(P_{2\mu})^2 + 1$, $u = 2P_{2\mu}Q_{2\mu}$ setzt.

Nun ist aber

$$\begin{aligned} P_{2\mu} &= (v, a, b \cdots l, m, m, l \cdots b, a) \\ &= (v, a, b \cdots l, m)(m, l \cdots b, a) + (v, a, b \cdots l)(l \cdots b, a) \\ &= (v, a, b \cdots l, m)(a, b \cdots l, m) + (v, a \cdots l)(a, b \cdots l) \\ &= P_{\mu+1}Q_{\mu+1} + P_\mu Q_\mu. \\ Q_{2\mu} &= (a, b \cdots l, m, m, l \cdots b, a) \\ &= (a, b \cdots l, m)(m, l \cdots b, a) + (a, b \cdots l)(l \cdots b, a) \\ &= (a, b \cdots l, m)(a, b \cdots l, m) + (a, b \cdots l)(a, b \cdots l) \\ &= (Q_{\mu+1})^2 + (Q_\mu)^2. \end{aligned}$$

II. Fall. Die Periode ist von gerader Gliederzahl. Sie heisse etwa

$$v, a, b \cdots k, l, m, l, k \cdots b, a \mid 2v$$

und

$$\frac{P_1}{Q_1};\ \frac{P_2}{Q_2} \cdots \frac{P_{\mu-2}}{Q_{\mu-2}};\ \frac{P_{\mu-1}}{Q_{\mu-1}};\ \frac{P_\mu}{Q_\mu};\ \frac{P_{\mu+1}}{Q_{\mu+1}} \cdots \frac{P_{2\mu-2}}{Q_{2\mu-2}};\ \frac{P_{2\mu-1}}{Q_{2\mu-1}}$$

seien die entsprechenden Näherungsbrüche. Dann ist

$$(P_{2\mu-1})^2 - D(Q_{2\mu-1})^2 = (-1)^{2\mu-2} = 1$$

und

$$\begin{aligned} P_{2\mu-1} &= (v, a, b \cdots k, l, m, l, k \cdots b, a) \\ &= (v, a, b \cdots l, m)(l, k \cdots b, a) + (v, a, b \cdots l)(k \cdots b, a) \\ &= (v \cdots m)(a \cdots l) + (v \cdots l)(a \cdots k) \\ &= P_{\mu+1}Q_\mu + P_\mu Q_{\mu-1}. \end{aligned}$$

$$\begin{aligned} Q_{2\mu-1} &= (a, b \cdots k, l, m, l, k \cdots b, a) \\ &= (a, b \cdots k, l, m)(l, k \cdots b, a) + (a, b \cdots k, l)(k \cdots a) \\ &= (a \cdots m)(a \cdots l) + (a \cdots l)(a \cdots k) \\ &= Q_{\mu+1} Q_\mu + Q_\mu Q_{\mu-1} \\ &= Q_\mu(Q_{\mu+1} + Q_{\mu-1}). \end{aligned}$$

Diese Bemerkung, welche die Rechnung fast um die Hälfte abkürzt, wurde von Tenner[1]) erneut veröffentlicht und daher vielfach[2]) diesem zugeschrieben.

Alles in allem genommen lässt das Eulersche Verfahren zur wirklichen Berechnung von Lösungen der Gleichung $t^2 - Du^2 = 1$ kaum etwas zu wünschen übrig, während allerdings die Beweise der Fundamentalsätze fehlen. Ich zähle diese Sätze nochmals auf.

1) Jede Quadratwurzel aus einer nicht quadratischen ganzen Zahl lässt sich in einen reinperiodischen Kettenbruch entwickeln.

2) Jede Periode schliesst mit dem Teilnenner $2v$.

3) Sätze über die Näherungsbrüche, vor allem $P^2 - Q^2D = (-1)^n \cdot \pi$ (π = Index zu P).

4) Der Nachweis, dass jede Auflösung p, q der Gleichung $t^2 - Du^2 = 1$ einen Näherungsbruch für $\sqrt{D}$ liefert.

In den folgenden Jahren erschienen Lagranges arithmethische Arbeiten. Doch sie waren, was unser Problem anlangt, ohne Einfluss auf Euler, ebenso wie Lagrange bei Abfassung seiner Abhandlung „Solution d'un problème d'arithmétique"[3]) die letztbesprochene Arbeit Eulers nicht gekannt zu haben scheint. Ich werde auf diesen letzteren Punkt noch einzugehen haben. Über den ersten sind wir besonders durch Briefe Lagranges und Eulers unterrichtet. Lagrange übersandte Euler seine Abhandlungen von 1770, vielleicht auch 1769 und 1768. Nachdem einige Briefe gewechselt sind, schreibt Euler[4]): „Je

---

1) Einige Bemerkungen über die Gleichung $t^2 - Du^2 = +1$ von G. W. Tenner. Programm Merseburg 1841. 4⁰.

2) z. B. Lehrbuch der unbestimmten Analytik von W. Berkhan. 2 Bde. 8⁰. Halle 1855 und 1856. Bd. II. Die Auflösung der Diophantischen Gleichungen 2. Grades. § 273. S. 177.

3) Lagrange, Solution d'un problème d'arithmétique. Miscellanea Taurinensia. Tome IV. 1766—1769. Oeuvres. Tome I. Paris 1867. p. 671. Le mémoire est daté de Berlin le 20. Sept. 1768.

4) Euler an Lagrange, 2. mars 1670 (Pétersbourg). Lagrange, Oeuvres. Bd. XIV. p. 219.

me suis fait lire toutes les opérations que vous avez faites sur la formule $1 = p^2 - 13q^2$ et je suis entièrement convaincu de leur solidité; mais étant hors d'état de lire ou d'écrire moi-même, je dois vous avouer, que mon imagination n'a pas été capable de saisir le fondement de toutes les déductions que vous avez été obligé de faire et encore moins de fixer dans mon esprit la signification de toutes les lettres, que vous y avez introduites. Il est bien vrai que de semblables recherches ont fait autrefois mes délices et m'ont coûté bien de temps; mais à présent je ne saurais plus entreprendre que celles, que je suis capable de développer dans ma tête et souvent je suis obligé de récourir à un ami pour exécuter les calculs que mon imagination projette".

Entsprechend drückt sich Lagrange gegenüber Condorcet aus[1]) „... je vous crois le seul qui m'ait fait cet honneur (seine Arbeiten zu lesen); car M. Euler, qui s'est beaucoup occupé autrefois de ce sujet et qui en a fait longtemps ses délices m'a mandé que la perte de sa vue ne lui ayant pas permis de lire mes Mémoires il n'avait cependant pas manqué de se les faire lire, mais qu'il lui avait été impossible de suivre mes raisonnements et mes calculs".

Schon bevor Lagrange diesen Brief schrieb, hatte Euler seine „Anleitung zur Algebra" herausgegeben.[2]) Er begnügt sich damit, in Kap. 7 die Wallissche Methode zur Auflösung der Gleichung $t^2 - Du^2 = 1$ darzustellen, ohne merkwürdigerweise von seinem 1765 gefundenen Algorithmus etwas zu erwähnen.

Auch die Zusätze zur Algebra, die Lagrange bald darauf herausgab und ihm übersandte, scheinen ohne Einfluss auf Euler geblieben zu sein, wenn man aus dem Antwortschreiben an Lagrange[3]) und aus der Thatsache schliessen darf, dass er in den beiden Abhandlungen,[4])

---

1) Lagrange an Condorcet, 30. Sept. 1771. Lagrange, Oeuvres. Bd. XIV. p. 230.

2) Leonhardt Eulers vollständige Anleitung zur Algebra. St. Petersburg 1771 bey der kaiserlichen Akademie der Wissenschaften. — Élémens d'algèbre par M. Léonard Euler, traduits de l'allemand avec des notes et des additions. Tome second: de l'analyse indeterminée. A Lyon chez Bruyset 1774. Die Übersetzung und die Zusätze zum ersten Teil sind von M. Bernouilli (à Berlin). Der zweite Teil enthält die „Additions" Lagranges. II. Aufl. Pétersbourg et Paris 1798.

3) Euler an Lagrange, 24. Sept. 1773. Lagrange, Oeuvres. Bd. XIV.

4) De resolutione irrationalium per fractiones continuas ubi simul nova quaedam et singularis species minime exponitur. Nov. Comm. XVIII. 1773. p. 218. Comm. arithm. coll. (I.) Pétersbourg 1849. p. 570. Hierzu auch Tschébyschev und Bouniakowsky ib. Einleitung. p. XLVII. Nr. 47.

in denen er sich noch mit der Fermatschen Gleichung beschäftigte, der „Additions" mit keinem Worte gedenkt.

Der letzte Aufsatz Eulers, der von der Gleichung $t^2 - Du^2 = 1$ handelt, ist, soviel ich sehe, die Abhandlung „Nova subsidia pro resolutione formulae $ax^2 + 1 = y^2$."[1]) In demselben stellt er eine Reihe Regeln auf, welche zur Konstruktion von Tabellen und zur Erleichterung der Rechnung dienen sollen. Da er jedoch auf eine Methode im Sinne der Fermatschen Aufgabe nicht eingeht, dürfen wir uns wohl mit der Aufzählung des Inhaltes der Schrift begnügen. Derselbe besteht:

1. Aus Regeln, aus Lösungen der Gleichungen

$$t^2 - Du^2 = -1,$$
$$t^2 - Du^2 = \pm 2,$$
$$t^2 - Du^2 = \pm 4,$$

solche der Gleichung

$$t^2 - Du^2 = 1$$

abzuleiten.

2. Aus Regeln, diejenigen Werte D zu bestimmen, für welche eine gegebene Zahl p als kleinste Lösung einer der obigen Gleichungen, und zwar an Stelle von u, möglich ist.

---

1) Nova subsidia pro resolutione formulae $ax^2 + 1 = y^2$. Euler, opusc. analytica. I. p. 310. Comm. arithm. coll. (II.) Pétersbourg 1849. p. 35.

III. Teil: Seit Lagrange.

§ 1. Lagrange.

Lagrange hat im Jahre 1768 begonnen, unserem Probleme seine Aufmerksamkeit zuzuwenden. Er schreibt am 15. August 1768 an d'Alembert:[1])

„Je me suis occupé, ces jours passés pour diversifier un peu mes études, de quelques problêmes d'Arithmétique et je vous assure, que j'ai trouvé beaucoup plus de difficulté, que je ne croyais. En voici un par exemple dont je ne suis venu à bout qu'avec beaucoup de peine: Un nombre quelconque donné, trouver un nombre entier et carré x^2 tel que $nx^2 + 1$ soit un carré. Ce problème est d'une grande importance dans la théorie des quantités carrés, qui font le principal objet de l'analyse de Diophante..... Au reste j'ai trouvé à cette occasion de très beaux théorèmes d'Arithmétique."

Die Resultate, von denen Lagrange hier spricht, wurden niedergelegt in der vom 20. September 1768 aus Berlin datierten Abhandlung „Solution d'un problème d'Arithmétique."[2]) Der Ausgangspunkt ist, ohne dass Lagrange die Eulersche Abhandlung vom Jahre 1765 gekannt hätte, der gleiche, wie bei diesem; doch ist der Weg, der eingeschlagen wird, ein anderer. Er empfindet vor allem den Mangel eines Nachweises, dass die Gleichung $t^2 - Du^2 = 1$ unter allen Umständen ganzzahlig lösbar sei, und dieser Beweis ist denn auch das Ziel, das er zunächst ins Auge fasst. Der Gang der Untersuchung ist etwa folgender:

I. Beweis, dass es stets ganze Zahlen giebt, welche die Gleichung $t^2 - Du^2 = 1$ befriedigen. Daraus fliessend eine Methode zur Ermittelung solcher Zahlen.

---

1) Lagrange an d'Alembert, 15. Aug. 1768. Oeuvres. Bd. XIII. p. 118.

2) Solution d'un problème d'arithmétique Miscellanea Taurinensia. Tome IV. 1766—1769. Oeuvres de Lagrange. Bd. I. Paris 1867. p. 671.

II. Formeln, aus einer Lösung weitere zu erhalten; Beweis, dass man mit Hilfe der angegebenen aus der kleinsten Lösung T, U alle anderen erhält.

III. Beweis, dass sich $\frac{T}{U}$ unter den Näherungsbrüchen für Kettenbruchentwicklung für $\sqrt{D}$ befindet; daraus eine zweite Methode der Lösung: man soll die Reihe der Näherungsbrüche für $\sqrt{D}$ bilden und successive die Zähler derselben an die Stelle von t, die Nenner statt u einsetzen, bis man $t^2 - Du^2 = 1$ erhält, was vermöge des Beweises I immer beliebig oft eintreten muss; nach welchem Gesetz, ist nicht ermittelt.

Obwohl sich in der Abhandlung alles vorfindet, was zu dem Nachweise nötig wäre, dass $\sqrt{D}$ in einen periodischen Kettenbruch entwickelt werden kann, wird dieser Satz doch nicht ausgesprochen.

I. Beweis, dass die Gleichung $t^2 - Du^2 = 1$ stets ganzzahlig lösbar sei.

Lagrange geht, wie früher Euler, von der Bemerkung aus, dass, wenn es zwei Zahlen giebt, welche der Bedingung $p^2 - Dq^2 = 1$ genügen, $\frac{p}{q}$ ein Näherungsbruch für $\sqrt{D}$ ist. Die Richtigkeit dieser Bemerkung wird jedoch erst später bewiesen und dient nur als Motiv zu dem folgenden Verfahren.

Bei demselben wird $\sqrt{D}$ in einen Kettenbruch mit positiven Teilnennern

$$\sqrt{D} = q + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cdots}}}$$

entwickelt und alsdann die Reihe der Näherungsbrüche

$$\frac{1}{0}\ \frac{M_1}{N_1}\ \frac{M_2}{N_2} \cdots\cdots \frac{M_k}{N_k} \text{ etc.}$$

berechnet. Die Nenner derselben werden an Stelle von u, die entsprechenden Zähler an Stelle von t in die Formel $t^2 - Du^2$ eingesetzt und so die Folge von Gleichungen

$$M_1{}^2 - DN_1{}^2 = Z_1$$

$$M_2{}^2 - DN_2{}^2 = Z_2$$

$$M_3{}^2 - DN_3{}^2 = Z_3 \quad \text{u. s. f.}$$
$$M_k{}^2 - DN_k{}^2 = Z_k \quad \text{etc.}$$

gewonnen, in welchen $Z_1 \ldots Z_\nu$ positive oder negative ganze Zahlen bezeichnen.

Nun wird nachgewiesen, dass der absolute Wert von Z_k

$$| Z_k | < \frac{2M_k}{N_k}.$$

Da aber die Brüche $\frac{M_k}{N_k}$ gegen den festen Wert $\sqrt{D}$ konvergieren, kann es nur eine endliche Zahl voneinander verschiedener Werte Z_k geben; nun lässt sich die Folge der Näherungsbrüche, somit der Gleichungen

$$M_k{}^2 - DN_k{}^2 = Z_k$$

beliebig weit fortsetzen; also müssen beliebig viele unter ihnen sein, die den gleichen Wert R liefern. Es seien etwa die folgenden:

$$x_1{}^2 - Dy_1{}^2 = R$$
$$x_2{}^2 - Dy_2{}^2 = R$$
$$x_\nu{}^2 - Dy_\nu{}^2 = R \quad \text{etc.},$$

wo x_ν und y_ν Zähler und Nenner des betreffenden Näherungsbruches bedeuten.

Machen wir einen Augenblick halt. Der Weg, den Euler von dem Punkte aus nahm, auf dem wir uns befinden und den auch Lagrange später wählte, ist der, nun die Grössen Z_ν zu untersuchen, ihre periodische Folge festzustellen und nachzuweisen, dass sich unter ihnen notwendig die Einheit befinden muss. Lagrange schlägt diesmal jedoch eine andere Richtung ein. Er benutzt dazu das schon den Indern bekannte[1]) und von ihnen bewiesene Lemma:

Aus

$$M_\nu^2 - DN_\nu^2 = Z_\nu$$
$$M_k^2 - DN_k^2 = Z_k$$

folgt durch Multiplikation

$$(M_\nu M_k \pm DN\, N_k)^2 - D\,(M_\nu N_k \pm M_\nu N_k)^2 = Z_\nu Z_k.$$

Mit Hilfe desselben zeigt er, dass man durch geeignete Multiplikation von Gleichungen der Folge

1) v. S. 20.

$$x_1^2 - Dy_1^2 = \pm R$$
$$x_2^2 - Dy_2^2 = \pm R \quad \text{etc.}$$

zu einer Gleichung

$$p^2 - Dq^2 = \pm R^{2\nu}$$

gelangen kann, in welcher p^2 und q^2 beide durch $R^{2\nu}$ teilbar sind.

Man hat alsdann

$$\left(\frac{p}{R^\nu}\right)^2 - D\left(\frac{q}{R^\nu}\right)^2 = \pm 1,$$

womit der gewünschte Nachweis erbracht wäre, da man von

$$t^2 - Du^2 = -1$$

durch Quadrieren leicht zu

$$(t^2 + Du^2)^2 - D(2tu)^2 = 1$$

gelangen kann.

Der Nachweis jedoch, dass man wirklich zu einer Gleichung

$$p^2 - Du^2 = R^{2\nu}$$

von der genannten Eigenschaft kommt, macht einige Schwierigkeit. Lagrange unterscheidet zwei Fälle, je nachdem R und D gemeinteilig sind oder nicht.

1. R und D nicht gemeinteilig.

Es kommt für den Beweis darauf an, aus wie vielen Primfaktoren R zusammengesetzt ist. Je nach ihrer Anzahl muss man gegebenenfalls verschieden viele Paare aus der Folge der Gleichungen

$$x_1^2 - Dy_1^2 = \pm R$$
$$x_2^2 - Dy_2^2 = \pm R \quad \text{etc.}$$

miteinander multiplizieren. Lagrange zeigt die Richtigkeit des behaupteten Satzes für die Fälle

(1) $R = P_1$

(2) $R = P_1 P_2$

(3) $R = P_1 P_2 P_3$

(4) $R = P_1 P_2 P_3 P_4$

(5) $R = P_1^n$,

wenn P_1 eine beliebige in D nicht aufgehende Primzahl bedeutet, indem in jedem Falle die Erledigung aller vorhergehenden vorausgesetzt wird.

Doch wird der ziemlich umständliche Beweis nicht auf den allgemeinen Fall

$$R = P_1^{n_1} P_2^{n_2} \dots P_6^{n_6}$$

ausgedehnt und nur bemerkt[1]): „On pourra abréger et simplifier de la même manière l'analyse des cas ou

$$R = P_1^{n_1} P_2^{n_2} \dots P_6^{n_6}$$

P_1, P_2 .... étant des nombres premiers".

Um eine Probe des Verfahrens zu geben, setze ich den Beweis für den einfachsten Fall $R = P_1$ und $R = P_1 P_2$ hierhin.

Aus

$$x_1^2 - Dy_1^2 = R,$$
$$x_2^2 - Dy_2^2 = R,$$

folgt nach dem Lemma

$$R^2 = (x_1 x_2 \pm D y_1 y_2)^2 - D(x_1 y_2 \pm y_1 x_2)^2$$

und durch Elimination von D

$$R(y_2^2 - y_1^2) = x_1^2 y_2^2 - y_1^2 x_2^2,$$

oder

$$R(y_2^2 - y_1^2) = (x_1 y_2 + y_1 x_2)(x_1 y_2 - y_2 x_1)$$

Es ist also

$$x_1 y_2 + y_2 x_1 \text{ oder } x_1 y_2 - y_1 x_2$$

durch R teilbar; dies möge durch

$$x_1 y_2 \pm y_2 x_1 = qR$$

angedeutet werden. Alsdann ist

$$R^2 = (x_1 x_2 \pm D y_1 y_2)^2 - D q^2 R^2,$$

somit also auch

$$x_1 x_2 \pm D y_1 y_2$$

durch R teilbar, und man erhält, wie behauptet

$$1 = p^2 - D q^2.$$

Ist $R = P_1 P_2$, so folgt wie eben

$$R^2 = (x_1 y_2 \pm D y_1 y_2)^2 - D(x_1 y_2 \pm y_1 x_2)^2,$$
$$R(y_2^2 - y_1^2) = (x_1 y_2 + y_1 x_2)(x_1 y_2 - y_1 x_2).$$

1) l. c. Art. 10. Oeuvres de Lagrange. Bd. I. p. 687, l. 6 von unten.

Nun gehen entweder $P_1 P_2$ gleichzeitig in einem der Faktoren rechts auf — was auf den vorigen Fall zurückführen und eine Lösung liefern würde — oder P_1 geht in den einen, P_2 in den anderen Faktor auf, so dass zum Beispiel

$$x_1 y_2 - y_1 x_2 = q P_2$$

ist, wo q durch P_1 nicht teilbar. Alsdann wird

$$P_1^2 P_2^2 = (x_1 x_2 - D y_1 y_2)^2 - D q^2 P_2^2,$$

somit auch $x_1 x_2 - D y_1 y_2$ durch P_2 teilbar, so dass

$$x_1 x_2 - D y_1 y_2 = p P_2$$

und

$$P_1^2 = p^2 - D q^2.$$

Es muss nun aber möglich sein, durch Multiplikation von

$$x_1^2 - D y_1^2 = R$$

mit einer anderen Gleichung etwa

$$x_\nu^2 - D y_\nu^2 = R$$

zu einer entsprechenden Gleichung

$$P_1^2 = p_1^2 - D q_1^2$$

zu gelangen. Denn entweder geht in der Gleichung

$$R(y_\nu^2 - y_1^2) = (x_1 y_\nu + x_\nu y_1)(x_1 y_\nu - x_\nu y_1)$$

einer der Faktoren rechts durch P_1 und P_2 auf; dann würde man sogleich nach dem zu erst erledigten Falle eine Lösung bekommen; oder P_1 geht nur in den einen, P_2 in den anderen Faktor auf, dann führt die gleiche Überlegung wie oben auf eine Gleichung

$$P_1^2 = p_1^2 - D q_1^2.$$

Aus den beiden Gleichungen

$$P_1^2 = p^2 - D q^2,$$
$$P_1^2 = p_1^2 - D q_1^2$$

ergiebt sich aber wie früher

$$P_1^4 = (p p_1 + D q q_1)^2 - D(p q_1 \pm q p_1)^2,$$
$$P_1^2 (q_1^2 - q^2) = (p q_1 + q p_1)(p q_1 - q p_1).$$

Es sei nun P_1 vorläufig nicht gleich 2. Aus der zweiten Gleichung folgt dann, dass $(pq_1 + qp_1)$ oder $(pq_1 - qp_1)$ durch P_1^2 teilbar sein müssen. Denn beide können sie durch P_1 nicht geteilt werden, da sonst auch ihre Summe, nämlich $2pq_1$, durch P_1 teilbar sein müsste, was der Voraussetzung widerspricht, dass weder p noch q_1 durch P_1 teilbar seien. Setzt man nun aber

$$pq_1 \pm qp_1 = sP_1^2,$$

wo dasjenige Zeichen gewählt werden muss, das $(pq_1 \pm qp_1)$ durch P_1^2 teilbar macht, so wird

$$P^4 = (pp_1 \pm Dqq_1)^2 - Ds^2 P_1^4,$$

also bei entsprechender Bedeutung des Doppelzeichens

$$pp_1 \pm Dqq_1 = rP_1^2$$

und also auch

$$1 = r^2 - Ds^2.$$

Ist $P_1 = 2$, so werden q und q_1 da sie beide relativ prim zu P_1, ungerade, ihre Quadrate also

$$\equiv 1 \ (mod\ 8)$$

oder

$$q_1^2 - q^2 = 8m.$$

Die Gleichung

$$P_1^2 (q_1^2 - q^2) = (pq_1 + p_1 q)(pq_1 - p_1 q)$$

verwandelt sich also in

$$32m = (pq_1 + p_1 q)(pq_1 - p_1 q);$$

einer der beiden Faktoren muss also zum mindesten durch 4, also P_1^2 teilbar sein. Man kann somit wie im vorigen Fall verfahren und erhält

$$1 = r^2 - Ds^2.$$

(2) R und D sind gemeinteilig.

(1a.) Ist der Teiler weder selbst ein Quadrat noch ein Multiplum eines Quadrates, so kann man durch Wegheben desselbigen aus der Gleichung

$$R = x_1^2 - Dy_1^2$$

und Quadrieren des Restes zu einer Gleichung $T^2 = p^2 - Dq^2$ gelangen, in welcher T^2 relativ prim zu D ist, und die somit nach den früheren Fällen erledigt werden kann.

(2a.) Ist der gemeinschaftliche Teiler von D und R ein Multiplum eines Quadrates, so erhält man nach Wegheben desselben eine Gleichung

$$\frac{R}{w^2} = p^2 - \frac{D}{w^2} q^2,$$

welche nach den gegebenen Regeln zu einer Lösung benutzt werden kann.

Es bleibt noch zur Vervollständigung des Beweises zu zeigen, dass man aus einer Lösung der Gleichung

$$1 = p^2 - \frac{D}{w^2} q^2$$

eine solche der Gleichung $1 = t^2 - Du^2$ ableiten kann, d. h. es bleibt noch zu zeigen, dass unter den Auflösungen $q_1 \ldots . q_n$ der Gleichung

$$1 = p^2 - \frac{D}{w^2} q^2$$

sich stets solche befinden, welche $\equiv o \ (mod\ w)$.

In der That liefert Lagrange diesen Nachweis am Schlusse der Arbeit in Artikel 21.

Sieht man von dem fehlenden Beweise für den Fall $R = P_1^{n_1} P_2^{n_2}$ etc. ab, so hat man hier zum ersten Male den strengen Nachweis der Lösbarkeit der Gleichung $t^2 - Du^2 = 1$ zugleich mit einer eigentümlichen Methode, Lösungen zu finden, wenn das Verfahren auch für jede spezielle Form von R besonderer Regeln bedarf.

In den meisten Fällen wird die Rechnung allerdings um die Hälfte kürzer, als wenn man fortfahren würde, Zähler und Nenner der Näherungsbrüche an Stelle von t und u in die Formel $t^2 - Du^2$ einzusetzen, bis $Z_\nu = +1$ würde.

Doch hat, wie wir gesehen haben, das abgekürzte Eulersche Verfahren den gleichen Vorzug.

II. Formeln, aus der kleinsten Lösung von $t^2 - Du^2 = 1$ alle übrigen abzuleiten.

Hat man zwei Zahlen p und q, so dass

$$p^2 - Dq^2 = 1,$$

so folgt

$$(p^2 - Dq^2)^m = (p + q\sqrt{D})^m (p - q\sqrt{D})^m = 1,$$

wenn m eine beliebige pos. ganze Zahl. Ferner ist

$$(p + q\sqrt{D})^m =$$

$$\Big\{p^m + \frac{m(m-1)}{1\cdot 2}p^{m-2}q^2D + \frac{m(m-1)(m-2)(m-3)}{1\cdot 2\cdot 3\cdot 4}p^{m-4}q^4D^2 + \text{etc.}\Big\}$$

$$+ \sqrt{D}\Big\{mp^{m-1}q + \frac{m(m-1)(m-2)}{1\cdot 2\cdot 3}p^{m-3}q^3D + \frac{m(m-1)(m-2)(m-3)(m-4)}{1\cdot 2\cdot 3\cdot 4\cdot 5}p^{m-5}q^5D^2 + \text{etc.}\Big\}$$

$$= x + y\sqrt{D}$$

und ebenso

$$(p - q\sqrt{D})^m = x - y\sqrt{D}.$$

Hieraus ergiebt sich

$$x = \frac{(p + q\sqrt{D})^m - (p - q\sqrt{D})^m}{2},$$

$$y = \frac{(p + q\sqrt{D})^m - (p - q\sqrt{D})^m}{2\sqrt{D}}$$

und

$$x^2 - Dy^2 = 1.$$

Aus der Berechnung folgt, dass x und y beide ganze Zahlen sind.

Man erhält somit aus einer von der selbstverständlichen Lösung $u = o$, $t = \pm 1$ verschiedenen Auflösung p, q beliebig viele andere, indem man in unserer Formel m alle positiven ganzen Zahlen durchlaufen lässt.

Es gilt zu zeigen, dass man alle möglichen Lösungen bekommt, wenn man für p q die kleinste Lösung T, U verwendet.

Lagrange führt den Nachweis so, dass er zeigt, dass man die nächst grössere Lösung erhält, indem man in der Formel oben $m = 2$ setzt, wieder die grössere durch $m = 3$ u. s. f.

Da der Beweis jedoch etwas umständlich ist, gebe ich ihn lieber in einer etwas abweichenden Form, im Anschluss an Dirichlet-Dedekind, um nicht nochmals auf den Gegenstand zurückkommen zu müssen.[1])

---

1) Dirichlet-Dedekind, Vorlesungen über Zahlentheorie. IV. Aufl. Braunschweig 1894. § 85. S. 211. Doch scheint mir der Beweis nicht vollständig, er gilt nur, wenn t' und u' positiv sind, und dass sie dies sind, muss erst bewiesen werden. Hierzu Disqu. Arithm. Art. 200.

Lemma. Sind t_*, u_* und t_n, u_n zwei positive Lösungen der Gleichung

$$t^2 - Du^2 = 1$$

und ist $u_n < u_*$, so ist auch

$$t^{(1)} = t_* t_n - u_* u_n D$$
$$u^{(1)} = u_* t_n - u_n t_*$$

eine aus positiven von o verschiedenen Zahlen bestehende Lösung derselben Gleichung.

Beweis. Erstens. Die Ausrechnung zeigt, dass vermöge der Voraussetzung

$$t_*^2 - Du_*^2 = 1; \qquad t_n^2 - Du_n^2 = 1$$

auch

$$t^{(1)2} - Du^{(1)2} = 1 \quad \text{ist.}$$

Zweitens.

(1) u^1 ist nicht o.

Denn aus $u^{(1)} = o$ oder

$$u_* t_n - t_* u_n = o$$

oder

$$\frac{t_*}{u_*} = \frac{t_n}{u_n}$$

folgt gegen die Voraussetzung

$$n_n < u_*$$
$$t_* = t_n, \qquad u_* = u_n,$$

weil vermöge der Gleichungen

$$t_*^2 - Du_*^2 = 1; \qquad t_n^2 - Du_n^2 = 1$$

t_n und u_n sowie t_* und u_* nicht gemeinteilige Zahlen sind.

(2) $u^{(1)}$ ist positiv.

Denn aus

$$t_n^2 - Du_n^2 = 1$$

und

$$t^2_* - Du^2_* = 1$$

folgt

$$\frac{t_n}{u_n} = \sqrt{D + \frac{1}{u_n^2}},$$

$$\frac{t_*}{u_*} = \sqrt{D + \frac{1}{u_*^2}}.$$

Da aber gemäss der Voraussetzung

$$u_n < u_*$$

wird

$$\frac{t_n}{u_n} > \frac{t_*}{u_*},$$

also

$$\frac{t_n}{u_n} - \frac{t_*}{u_*} > 0$$

und

$$t_n u_* - t_* u_n > 0 \quad \text{q. e. d.}$$

Drittens.

(1) $t^{(1)}$ ist nicht 0, da $t^{(1)2} - D u^{(1)2} = 1$

(2) $t^{(1)}$ ist positiv.

Aus

$$t^{(1)} = t_* t_n - u_* u_n D$$

folgt

$$\frac{t_n t_*}{u_n u_*} - D = \frac{t^{(1)}}{u_n u_*},$$

da aber

$$\frac{t_n^2}{u_n^2} = D + \frac{1}{u_n^2},$$

$$\frac{t_*^2}{u_*^2} = D + \frac{1}{u_*^2}$$

erhält man

$$\frac{t_n t_*}{u_n u_*} = \sqrt{D^2 + D\left(\frac{1}{u_n^2} + \frac{1}{u_*^2}\right) + \frac{1}{u_n^2 u_*^2}},$$

wo die Wurzel positiv zu nehmen, da $t_n t_*$, $u_n u_*$ als positiv vorausgesetzt werden. Da ebenso alle Grössen unter der Wurzel positiv, so folgt

$$\frac{t_n t_*}{u_n u_*} > D,$$

also

$$\frac{t^{(1)}}{u_n u_*} = \frac{t_n t_*}{u_n u_*} - D > 0$$

und da $u_n u_*$ positiv

$$t^{(1)} > 0 \quad \text{q. e. d.}$$

Mit Hilfe des soeben bewiesenen Lemmas zeigen wir nun, dass die Formel $(T + U\sqrt{D})^m = t_m + u_m\sqrt{D}$, in welcher T, U die kleinste positive Auflösung der Gleichung $t^2 - Du^2 = 1$ bezeichnet, alle Auflösungen $+ t_m$, $+ u_m$ der nämlichen Gleichung liefert.

Beweis. Wie schon gezeigt, ist

$$t_m{}^2 + Du_m{}^2 = 1.$$

Es folgt

$$\frac{t_m}{u_m} = \sqrt{D + \frac{1}{u_m{}^2}}.$$

Es wachsen also t_m und u_m gleichzeitig, wenn man m grössere Werte verleiht. Daher bilden die Grössen

$$(T + U\sqrt{D});\quad (t_1 + u_1\sqrt{D}) \cdots (t_m + u_m\sqrt{D})$$

eine beständig wachsende Reihe.

Nehmen wir an, es gäbe eine aus positiven Zahlen t_*, u_* bestehende Auflösung der Gleichung $t^2 - Du^2 = 1$, welche nicht in unserer Formel enthalten sei. Dann muss $t_* + u_*\sqrt{D}$ notwendig zwischen zwei auf einander folgende Glieder der Reihe

$$(T + U\sqrt{D}) \cdots (t_m + u_m\sqrt{D})$$

fallen, so dass etwa

$$t_n + u_n\sqrt{D} < t_* + u_*\sqrt{D} < t_{n+1} + u_{n+1}\sqrt{D}$$

oder zufolge des Bildungsgesetzes der Grössen $t_k + u_k\sqrt{D}$

$$t_n + u_n\sqrt{D} < t_* + u_*\sqrt{D} < (t_n + u_n\sqrt{D})(T + U\sqrt{D}).$$

Multipliziert man die ganze Ungleichung mit $t_n - u_n\sqrt{D}$, so kommt

$$1 < t^{(1)} + u^{(1)}\sqrt{D} < T + U\sqrt{D},$$

wo

$$t^{(1)} = t_* t_n - u_* n_n D,$$
$$u^{(1)} = u_* t_n - t_* u_n.$$

Zufolge des Lemmas sind aber $t^{(1)}$ und $u^{(1)}$ positive ganze Zahlen; man würde also entgegen der Voraussetzung, dass T, U die kleinste Lösung sei, $t^{(1)} + u^{(1)}\sqrt{D} < T + U\sqrt{D}$ zum mindesten also

$$t^{(1)} < T$$

und daher auch

$$u^{(1)} < U$$

haben. Es muss also auch u_* und t_* in der Reihe der Grössen t_1, u_1 bis t_n, u_n enthalten sein, da die gegenteilige Annahme auf einen Widerspruch führt.

Unsere Formel liefert also alle Auflösungen in positiven Zahlen. Durch Vertauschung der Vorzeichen bekommt man hieraus sämtliche.

III. führt Lagrange in Nr. 18 der in Rede stehenden Abhandlung einen ziemlich umständlichen Beweis, dass $\frac{p}{q}$ sich unter den Näherungsbrüchen der Kettenbruchentwicklung für $\sqrt{D}$ befindet, wenn $p^2 - Dq^2 = 1$, indem er zeigt, dass die Annahme, $\frac{p}{q}$ liege zwischen zwei auf einander folgenden Näherungsbrüchen $\frac{M_k}{N_k}$ und $\frac{M_{k+1}}{N_{k+1}}$, so dass

$$M_k < p < M_{k+1}$$
$$N_k < q < N_{k+1}$$

auf einen Widerspruch führt.

Man brauche also nur Zähler und Nenner der successiven Näherungsbrüche in die Formel

$$t^2 - Du^2 = x$$

einzusetzen, um sicher einmal einen Wert $x = 1$ zu erhalten, und hiermit sei eine zweite Methode gegeben, die Gleichung

$$t^2 - Du^2 = 1$$

aufzulösen.

Dies ist in Kürze der Gang der Untersuchung, der man, scheint mir, namentlich im dritten Abschnitt (nach unserer Einteilung) anmerkt, dass Lagrange die Eulersche Abhandlung „de usu novi algorithmi" noch nicht kannte. Doch will das gegenüber der Thatsache wenig besagen, dass zum ersten Mal ein strenger Beweis der Lösbarkeit der Gleichung $t^2 - Du^2 = 1$ erbracht wird, und ich erinnere nur an das, was Gauss in seiner Anzeige des Seeberschen Werkes über den Gesichtspunkt sagt, aus welchem Beweise wie der hier von Lagrange erbrachte beurteilt sein wollen.

Lagrange selbst war von seiner Arbeit nicht völlig befriedigt. So sagt er in den „Additions“ [1])

„. . . . mais elle est très-longue et très-indirecte“

und in der Schrift „Sur la solution des problèmes indeterminées du second degré [2])

„. . . . ce que je n'avais pu démontrer alors que par un assez long circuit“.

Schon in der Abhandlung, der wir diese Worte entnehmen und welche wenige Monate nach jener ersten vollendet wurde [2]), beschäftigte er sich aufs neue mit unserem Problem; diesmal jedoch von einem anderen Standpunkt aus. Es ist hervorzuheben, dass Lagrange auch jetzt noch nicht den Aufsatz Eulers vom Jahre 1765 kennt.

Der Gang der Untersuchung — soweit sie unsere Gleichung betrifft — ist etwa folgender:

Das Problem, von welchem ausgegangen wird, ist die Lösung der allgemeinen unbestimmten biquadratischen Gleichung in ganzen Zahlen.

Diese Aufgabe reduziert sich auf die der Lösung einer Gleichung

$$A = t^2 - Du^2.$$

Die Gleichung $1 = t^2 - Du^2$ wird als spezieller Fall dieser allgemeineren aufgefasst und mit Hilfe der Methoden aufgelöst, welche für diese entwickelt wurden.

Wir wollen D als positiv und ohne quadratischen Teiler mit A voraussetzen.

1) Lagrange zeigt, dass man nun t, u; u, A; t, A als relative Primzahlen voraussetzen darf,

2) dass D quadratischer Rest zu A sein muss, damit die Gleichung

$$A = t^2 - Du^2$$

lösbar sei, dass diese Bedingung jedoch nicht ausreicht,

1) Additions aux élémens d'algèbre d'Euler; zum ersten Mal gedruckt als Anhang zu Élémens d'algèbre par M. L. Euler traduits de l'Allemand. Tome II. Lyon chez Bruyset 1774. p. 371 u. f.; verbessert. ib. II. Ausgabe. Paris 1798; hiernach in Lagrange, Oeuvres. Bd. VII. Paris 1877. Seite 158.

2) Sur la solution des problèmes indeterminées du second degré. Lu dans l'académie de Berlin le 24. Nov. 1768. Mém. de l'académie roy. des sc. de Berlin. Tome 23. 1769. Lagrange, Oeuvres. Tome II. Paris 1868. p. 396 l. 3 von unten. — Hierzu auch die Anzeige in dem Brief an d'Alembert vom 6. Dez. 1768. Lagrange, Oeuvres. Tome 13. p. 123.

3) dass sich jede Gleichung, wenn sie möglich und wenn $|A| > \sqrt{D}$, zurückführen lässt auf eine solche, wo $|A| < \sqrt{D}$,

4) wird ein Verfahren entwickelt, um zu entscheiden, ob die reduzierte Gleichung eine Lösung in ganzen Zahlen zulässt; ist dies der Fall, so giebt die Methode gleichzeitig eine Lösung,

5) wird gelehrt, wie man aus einer dieser Lösungen alle finden könne.

Die Bedingungen 1, 2, 3 sind bei unserer Gleichung schon von selbst erfüllt da, wenn

$$1 = t^2 - Du^2,$$

D quadratischer Rest zu 1, t und u relative Primzahlen und $1 < \sqrt{D}$. Die Aufgabe unter 5 ist bereits bei Gelegenheit der vorigen Abhandlung Lagranges allgemein erledigt worden. Es erübrigt somit nur das Verfahren 4 auseinanderzusetzen. Da jedoch das Reduktionsverfahren 3 eng mit der Methode 4 verknüpft ist und auch in anderer Hinsicht für unsere Aufgabe besonderes Interesse gewährt, so soll der Gang desselben im folgenden kurz gedeutet werden.

Wir wollen annehmen, man habe zwei nicht gemeinteilige Zahlen p, q, so dass

$$A = p^2 - Dq^2, \quad |A| > \sqrt{D}$$

und A und D ebenfalls nicht gemeinteilig. Dann lassen sich zwei Zahlen p_1, q_1 so finden, dass

$$qp_1 - pq_1 = \mp 1.$$

Man bildet

$$p_1{}^2 - Dq_1{}^2 = A_1$$

nnd multipliziert die Gleichung

$$A = p^2 - Dq^2$$

auf beiden Seiten damit. Das giebt

$$A(p_1{}^2 - Dq_1{}^2) = (pp_1 - Dqq_1)^2 - D$$

oder

$$AA_1 = \alpha^2 - D.$$

Da nun aber vermöge der Gleichung $qp_1 - pq_1 = \pm 1$,

$$p_1 = \mu p \pm m, \quad q_1 = \mu q \pm n,$$

wo μ eine beliebige ganze Zahl, so erhält man

$$\alpha = \mu(p^2 - Dq^2) \pm (pm - Dqn)$$

oder

$$a = \mu A \pm a, \qquad a < A;$$

man kann sich alsdann mit μ so einrichten, dass $a < \frac{A}{2}$. Berücksichtigt man dies in der Gleichung

$$A A_1 = a^2 - D,$$

so ergiebt sich $A_1 < \frac{A}{4}$.

Da man aber mit Hilfe der Gleichungen

$$qp_1 - pq_1 = \mp 1$$
$$pp_1 - qq_1 D = a$$

leicht von einer Lösung der Gleichung

$$p_1{}^2 - Dq_1{}^2 = A_1$$

auf eine solche der Gleichung

$$p^2 - Dq^2 = A$$

zurückgelangen kann, so ist die Aufgabe der Auflösung dieser letzteren reduziert auf die der ersten Gleichung $p_1{}^2 - Dq_1{}^2 = A_1$ in welcher $|A_1| < |A|$. Ist nun $|A_1| < \sqrt{D}$, so sind wir am Ziele; anderenfalls leuchtet ein, dass man mit der Gleichung

$$A_1 = p_1{}^2 - Dq_1{}^2$$

in vollkommen entsprechender Weise verfahren kann und so fort, bis man zu einer Gleichung $A_\nu = p_\nu{}^2 - Dq_\nu{}^2$ kommt, in welcher $|A_\nu| < \sqrt{D}$.

Man hat also folgendes Reduktionsschema, wenn p und q bekannt

$$\begin{array}{lll} A = p^2 - Dq^2 & pq_1 - qp_1 = \mp 1 & a = \mu A \mp a \\ A_1 = p_1{}^2 - Dq_1{}^2 & p_1 q_2 - q_1 p_2 = \mp 1 & a_1 = \mu_1 A_1 \mp a_1 \\ A_2 = p_2{}^2 - Dq_2{}^2 & p_2 q_3 - q_2 p_3 = \mp 1 & a_2 = \mu_2 A_2 \mp a_2 \end{array}$$

$$a < \frac{A}{2} \qquad A A_1 = a^2 - D$$

$$a_1 < \frac{A_1}{2} \qquad A_1 A_2 = a_1{}^2 - D$$

$$a_2 < \frac{A_2}{2} \qquad A_2 A_3 = a_2{}^2 - D \text{ etc.}$$

Da aus der Voraussetzung, die Gleichung $A = p^2 - Dq^2$ sei durch die Zahlen p, q erfüllt, folgt, dass D quadratischer Rest zu sämtlichen A, so muss dies letztere auch umgekehrt notwendige Voraussetzung der Lösbarkeit der Gleichung $A = p^2 - Dq^2$ sein.

Wir lassen jetzt die Annahme, dass p und q bekannt seien, fallen. Dann lässt sich die Reduktion offenbar nach folgendem Schema ausführen

$$AA_1 = \alpha^2 - D, \quad \text{wo} \quad \alpha < \left|\frac{A}{2}\right| \quad \text{gewählt wird}$$

$$A_1 A_2 = \alpha_1{}^2 - D, \quad \text{wo} \quad \alpha_1 \text{ resp. } \mu_1 A_1 + \alpha < \left|\frac{A_1}{2}\right| \quad \text{,, \quad ,,}$$

$$A_2 A_3 = \alpha_2{}^2 - D, \quad \text{wo} \quad \alpha_2 \quad \text{,,} \quad \mu_2 A_2 + \alpha_1 < \left|\frac{A_2}{2}\right| \quad \text{,, \quad ,, \quad etc.}$$

Ist die Gleichung $t^2 - Du^2 = A$ möglich, so lassen sich in der That, wie oben gezeigt, stets alle α finden, man wird sogar im allgemeinen für jedes α mehrere verschiedene Werte wählen können. Doch übergehe ich der Kürze wegen diese Angelegenheit.

Jedenfalls wird man auf dem bezeichneten Wege, welchen der verschiedenen Werte für jedes α_ν man auch wählen mag, stets, sofern die Gleichung $A = p^2 - Dq^2$ nur möglich ist, zu einer Gleichung $A_n = p_n{}^2 - Dq_n{}^2$ gelangen, in welcher $|A_n| < \sqrt{D}$; hat man diese aufgelöst, kennt also A_n, p_n und q_n, sowie

$$\alpha^2_{n-1} = A_{n-1} A_n + D,$$

so kann man mit Hilfe der Formeln

$$p_{n-1} = \frac{\alpha_{n-1} p_n + D q_n}{A_n},$$

$$q_{n-1} = \frac{\alpha_{n-1} q_n \pm p_n}{A_n},$$

welche aus den Gleichungen

$$p_{n-1} q_n - q_{n-1} p_n = \pm 1,$$

$$p_{n-1} q_n - D q_{n-1} q_n = \alpha_{n-1}$$

folgen, zu einer Lösung p, q der Gleichung

$$p^2 - Dq^2 = A$$

zurücksteigen.

Wir haben schon früher des Vergleiches gedacht (S. 26), welchen Hankel zwischen dem indischen Verfahren und dem soeben vorgetragenen

ausführt. In der That sind beide nahezu identisch, nur dass der Weg von den bekannten zu den zu findenden Grössen der umgekehrte ist. Die indische Regel war:

Man wähle 2 beliebige nicht gemeinteilige Zahlen p, q und setze sie in die Formel $t^2 - Du^2$ ein; dann erhält man $A = p^2 - Dq^2$. Dann bestimme man α so, dass $\alpha^2 - D$ möglichst klein und $q_1 = \frac{p + q\alpha}{A}$ ganzzahlig wird, setze

$$A_1 = \frac{\alpha^2 - D}{A} \quad \text{und} \quad p_1 = \frac{pq_1 - 1}{q},$$

alsdann ist, so wird gezeigt, in ganzen Zahlen,

$$A_1 = p_1^{\,2} - Dq_1^{\,2}.$$

Aus dem Lagrangeschen Verfahren folgt aber die nämliche Regel. Denn aus den Gleichungen

$$pq_1 - qp_1 = \pm 1$$
$$pp_1 - Dqq_1 = \alpha$$

ergiebt sich

$$q_1 = \frac{p + q\alpha}{\pm A}, \quad p_1 = \frac{pq_1 \pm 1}{q}$$

und ebenso ist $A_1 = \frac{\alpha^2 - D}{A}$.

Von dem Punkte an, wo eine Gleichung $A_n = q_n - Dq_n$ erreicht ist, in welcher $| A_n | < \sqrt{D}$, unterscheiden sich beide Verfahren, nämlich das indische und das von Lagrange, in der Form ein wenig, wenn auch nicht in der Sache.

Das indische Verfahren geht wie bisher weiter, nur dass es jetzt nicht mehr gerade möglich ist, $A_{n+1} < A_n$ zu erhalten. Doch wird man es genau wie bisher bewirken können, dass die Grössen $| A_{n+\lambda} |$ zum mindesten abwechselnd $< \sqrt{D}$ sind. Daraus folgt aber, wie bei Lagrange, dass nun alle $| A_{n+\mu} | < D$ sind, mit den Vorzeichen abwechseln und in periodischer Folge wiederkehren. Unter ihnen befindet sich die Einheit und man gelangt somit thatsächlich, wie die Inder wollten, zu einer Lösung der Gleichung $t^2 - Du^2 = 1$.

Der Beweis freilich, dass dem so ist, bildet, wie mir scheint, eine Hauptschwierigkeit, die vielleicht für Lagrange die Veranlassung war, den direkten Weg zu verlassen, welchen die Inder einhalten. Dazu trug jedenfalls jedoch auch die Verschiedenheit der Zwecke bei.

Denn während die Inder von den bekannten anfänglich gewählten Zahlen p, q ausgehen, somit stets mit bekannten Grössen operieren und am Ziele sind, sobald die Gleichung $p^2_{n+\lambda} - q^2_{n+\lambda} D = 1$ erscheint, ist damit für Lagrange, der von der zu lösenden Gleichung $p^2 - Du^2 = A$ ausgeht, an und für sich noch nichts gewonnen, und er muss aus den bei dem Reduktionsverfahren benutzten Grössen heraus nun einen Algorithmus finden, eine der Gleichungen aus der Kette

$$p^2 - Dq^2 = A \quad \text{bis} \quad p^2_{n+\lambda} - q^2_{n+\lambda} D = 1$$

aufzulösen.

Zu diesem Ende ruft er, in ähnlicher Weise, wie in seiner ersten Abhandlung die Kettenbruchentwicklung von $\frac{p_n}{q_n}$ zu Hilfe, nur dass er diesmal die damals verschmähte Richtung einschlägt, die früher Z_ν genannten Grössen einer genaueren Untersuchung zu unterziehen.

Wir waren bis zu der Gleichung

$$A_n = p_n^2 - Dq_n^2$$

gelangt, wo $A_n < \sqrt{D}$ und

$$A_n A_{n+1} = \alpha_n^2 - D; \quad \alpha_n = \mu_n A_n + \alpha_{n-1} < \left|\frac{A_n}{2}\right|.$$

Daraus folgt aber, dass

$$\alpha_n^2 < D, \ |\alpha_n| < \sqrt{D},$$

somit

$$-A_n A_{n+1} = D - \alpha_n^2 > 0.$$

Es haben also A_n und A_{n+1} entgegengesetzte Zeichen. Nennen wir $A_n \cdots \pm E$, so wird $A_{n+1} = \mp F$ sein und die Aufgabe ist, die Gleichung

$$\pm E = r^2 - Ds^2$$

aufzulösen.

Nehmen wir an, es gäbe zwei relative Primzahlen r und s, welche diese Gleichung befriedigen, dann kann man $\frac{r}{s}$ in den endlichen Kettenbruch

$$\frac{r}{s} = \alpha + \cfrac{1}{\beta + \cfrac{1}{\gamma + \cfrac{1}{\delta + \cdots \, + \cfrac{1}{w}}}}$$

entwickeln, wo $w \geqq 2$. Die Näherungsbrüche seien

$$\frac{1}{0}, \frac{a}{b} \cdots \frac{m}{n}, \frac{r}{s}.$$

Nennen wir sie in umgekehrte Folge genommen

$$\frac{r}{s}, \frac{r_1}{s_1} \cdots \frac{1}{0}$$

und die zugehörigen Teilnenner

$$\lambda_1, \lambda_2 \cdots \text{etc.},$$

so wird, je nachdem die Näherungsbrüche in gerader oder ungerader Anzahl vorhanden

$$rs_1 - r_1 s = \pm 1$$
$$r_1 s_2 - r_2 s_1 = \pm 1 \text{ etc.}$$

und

$$r = \lambda_1 r_1 + r_2 \qquad s = \lambda_1 s_1 + s_2$$
$$r_1 = \lambda_2 r_2 + r_3 \qquad s_1 = \lambda_2 s_2 + s_3$$
$$r_2 = \lambda_3 r_3 + r_4 \text{ etc.} \qquad s_2 = \lambda_3 s_3 + s_4 \text{ etc.}$$
$$r > r_1 > \cdots > 1 > 0$$
$$s > s_1 > \cdots > 0.$$

Setzt man nun die Grössen r_ν, s_ν resp. an die Stelle von t und u in die Formel $t^2 - Du^2$ ein, so erhält man, bei gleicher Bedeutung von $\pm$

$$\pm E = r^2 - Ds^2$$
$$\mp E_1 = r^2_1 - Ds^2_1$$
$$\pm E_2 = r^2_2 - Ds^2_2 \text{ etc.},$$

wo alle E_ν positive Zahlen sind.

Multipliziert man je zwei auf einander folgende Gleichungen und nennt

$$rr_1 - ss_1 D = + \varepsilon \text{ (das Zeichen wie eben)},$$
$$r_1 r_2 - s_1 s_2 D = \pm \varepsilon_1 \text{ etc.},$$

so kommt

$$EE_1 = D - \varepsilon^2,$$
$$E_1 E_2 = D - \varepsilon^2_1,$$
$$E_2 E_3 = D - \varepsilon^2_2 \text{ etc.}$$

Berücksichtigt man ferner, dass

$$r_{\varrho-1} = r_\varrho \lambda_\varrho + r_{\varrho+1}, \qquad s_{\varrho-1} = s_\varrho \lambda_\varrho + s_{\varrho+1},$$

so erhält man:

$$\varepsilon_\varrho = \lambda_\varrho E_\varrho - \varepsilon_{\varrho-1},$$

also

$$\varepsilon_1 = \lambda_1 E_1 - \varepsilon,$$

$$\varepsilon_2 = \lambda_2 E_2 - \varepsilon_1 \text{ etc.},$$

die nämlichen Gleichungsfolgen, die gekommen sein würden, falls man nach dem indischen Verfahren weitergegangen wäre.

Da alle E positiv, müssen alle

$$\varepsilon_\nu^2 < D$$

sein. Wie **Lagrange** zeigt und wie leicht aus dem Lemma S. 68 hervorgeht, sind zugleich alle ε positiv. Nun ist

$$\varepsilon < \sqrt{D}, \qquad \varepsilon > \sqrt{D} - E.[1]$$

Mit Hilfe dieser Ungleichungen kann man aber die Zahlen λ_1 etc. bestimmen, denn es folgt aus ihnen[2])

$$\frac{\sqrt{D} + \varepsilon}{E_1} - 1 < \lambda_1 < \frac{\sqrt{D} + \varepsilon}{E_1},$$

$$\frac{\sqrt{D} + \varepsilon_1}{E_2} - 1 < \lambda_2 < \frac{\sqrt{D} + \varepsilon_1}{E_2},$$

$$\frac{\sqrt{D} + \varepsilon_2}{E_3} - 1 < \lambda_3 < \frac{\sqrt{D} + \varepsilon_2}{E_3} \text{ etc.},$$

wodurch die λ unzweideutig festgelegt werden. Durch jedes λ wird aber ein Näherungsbruch bestimmt, sobald man einen aus der Reihe der $\frac{r_k}{s_k}$ kennt. Dies wird der Fall sein, wenn man bis zu $r_\varrho = 1$, $s_\varrho = 0$ gelangt ist. Und umgekehrt muss man, wenn es eine Lösung giebt, stets zu einem Wert $r_\varrho = 1$, $s_\varrho = 0$ gelangen können. Aus der Gleichung

$$r_\varrho^2 - s_\varrho^2 D = \pm E_\varrho$$

folgt dann, dass $E_\varrho = \pm 1$, je nachdem ϱ gerade oder ungerade.

Die Grössen λ etc. können nun aber beliebig fortgesetzt werden. **Lagrange** zeigt, dass sie ebenso, wie die E_ϱ und ε_ν sich periodisch wiederholen müssen, und liefert so, ohne es auszusprechen, den Beweis,

1) Vergl. **Lagrange**, l. c. S. 432. Art. 33.

2) **Lagrange**, ib. p. 433.

dass sich jede Wurzel einer quadratischen Gleichung in einen periodischen Kettenbruch entwickeln lässt.

Dazu zeigt er, 1) dass zwei auf einander folgende Zahlen E_ϱ, $E_{\varrho+1}$ alle vorhergehenden und nachfolgenden E bestimmen. Denn aus

$$E_\varrho E_{\varrho+1} = D - \varepsilon_\varrho^2$$

erhält man ε_ϱ, aus

$$E_{\varrho-1} E_\varrho = D - \varepsilon_{\varrho-1}^2,$$

$E_{\varrho-1}$, da

$$\varepsilon_\varrho = \lambda_\varrho E_\varrho - \varepsilon_{\varrho-1}$$

$\varepsilon_{\varrho-1}$ giebt, weil λ_ϱ durch die Bedingung

$$\frac{\sqrt{D} + \varepsilon_\varrho}{E_\varrho} < \lambda_\varrho < \frac{\sqrt{D} + \varepsilon_\varrho}{E_\varrho}$$

bekannt ist, die sich, wie Lagrange zeigt, gleichfalls leicht aus den Gleichungen Seite 78 ableiten lässt.

In der anderen Richtung war

$$\frac{\sqrt{D} + \varepsilon_\varrho}{E_{\varrho+1}} - 1 < \lambda_{\varrho+1} < \frac{\sqrt{D} + \varepsilon_\varrho}{E_{\varrho+1}},$$

also

$$\varepsilon_{\varrho+1} = \lambda_{\varrho+1} E_{\varrho+1} - \varepsilon_\varrho$$

und es ist somit $E_{\varrho+2}$ durch

$$E_{\varrho+1} E_{\varrho+2} = D - \varepsilon_{\varrho+1}^2$$

bestimmt etc.

2) sind alle positiven Zahlen $E < D$ vermöge der Gleichungen

$$E_\varrho E_{\varrho+1} = D - \varepsilon_\varrho^2;$$

es giebt ihrer also nur eine begrenzte Zahl, folglich auch nur eine begrenzte Zahl von Kombinationen zu je zweien. Eine solche muss also notwendig beliebig oft wiederkehren, wenn man die Reihe der E beliebig weit fortsetzt, und da, wie gezeigt, je zwei auf einander folgende $E_\varrho E_{\varrho+1}$ alle folgenden und vorhergehenden E bestimmt, so müssen sich gleiche Gruppen derselben wiederholen und E von allen E_ϱ zuerst wiederkehren.

Nach alledem gestaltet sich die Auflösung der Gleichung $A = t^2 - Du^2$ folgendermassen, wenn $|A| > \sqrt{D}$

1) Reduktion der Gleichung $A = t^2 - Du^2$ auf die Gleichung $\pm E = r^2 - Ds^2$, wo $E < \sqrt{D}$. Ist diese Reduktion nicht möglich, so ist auch die erste Gleichung nicht möglich.

2) Bildung von ε nach der Vorschrift $\varepsilon < \sqrt{D}$, $\varepsilon > \sqrt{D} - E$, $D - \varepsilon^2$ durch E teilbar. Ist dies nicht möglich, so ist auch die Gleichung $E = r^2 - Ds^2$, also auch $A = t^2 - Du^2$ nicht möglich.

3) Bildung der λ_ϱ, ε_ϱ und E_ϱ nach dem früheren Schema, bis E zum zweiten Mal wiederkehrt. Hat man keine Zahl $E_\mu = 1$ gefunden, so ist das Problem unmöglich. Im entgegengesetzten Fall bildet man mit Hilfe der bis zur Stelle $E_\mu = 1$ gefundenen Grössen λ und mit Hilfe der beiden symbolischen Näherungsbrüche $\frac{0}{1}, \frac{1}{0}$ die Reihe der folgenden. Der letzte ist eine Lösung von

$$E = p^2 - Ds^2,$$

und von dieser Gleichung aus gelangt man auf dem früher angegebenen Wege zu einer Lösung von

$$A = t^2 - Du^2.$$

Auf die Frage, wie man aus einer Lösung dieser Gleichung alle finden kann, gehe ich hier nicht ein, da wir das Problem, soweit es unsere Gleichung $t^2 - Du^2 = 1$ betrifft, bereits völlig gelöst haben.

Die Anwendung der oben entwickelten Methode auf die Fermatsche Gleichung ergiebt sich ohne Schwierigkeit:

1) Da D stets quadratischer Rest zu 1, ferner $1 < \sqrt{D}$, ist die Methode anwendbar.

2) Die Gleichung $t^2 - Du^2 = 1$ ist stets möglich. Denn da man stets zwei Zahlen ohne gemeinsamen Teiler p, q wählen kann, so dass etwa

$$p^2 - Dq^2 = A$$

(wo A das Resultat des Einsetzens), wird man nach dem Lagrangeschen Reduktionsverfahren stets auf beliebig viele Gleichungen

$$A = r^2{}_{n+\mu\varrho} - Ds^2{}_{n+\mu\varrho}$$

kommen, deren letztgewählte man durch die Annahme $r_{n+\mu\varrho} = 1$, $s_{n+\mu\varrho} = 0$ befriedigt. Die vorhergehenden werden dann durch die von 0 verschiedenen Werte;

$$r_{n+\mu-\overline{1\varrho}}; \quad s_{n+\mu-\overline{1\varrho}} \text{ etc.}$$

erfüllt. Die Gleichung $t^2 - Du^2 = 1$ ist also für jeden Wert von D in ganzen Zahlen lösbar.

Noch einfacher folgt das nämliche aus dem Umstande, dass E, welches die Periode beginnt und in unserem Falle gleich der Einheit ist, beliebig oft wiederkehren muss.

3) Es giebt nur ein ε, so dass

$$\sqrt{D} - 1 < \varepsilon < \sqrt{D};$$

dies ist die grösste ganze Zahl in $\sqrt{D}$. Man kann also das Verfahren der Bestimmung der λ, E, ε, das, wie man sieht, mit der Entwicklung von $\sqrt{D}$ in einen Kettenbruch identisch ist, ausführen; jedes E, welches gleich der Einheit wird, liefert eine Lösung. Aus den Voraussetzungen des Verfahrens folgt weiter, dass man so jede Lösung erhalten muss, und da die Werte für t und u mit der Anzahl der benutzten λ wachsen, muss diejenige Lösung, welche man an der erstmöglichen Stelle erhalten hat, zugleich die kleinste sein.

Zum Schlusse dieser Besprechung füge ich noch eine Formel Lagranges bei, welche auch auf das in dem ersten Aufsatze geübte Multiplikationsverfahren ein Licht wirft.

Hat man die kleinsten Auflösungen T, U gefunden, so dass

$$T^2 - DU^2 = \pm 1,$$

so kann man folgende Umformung vornehmen. μ soll ein Multiplum der Periodenanzahl sein, gerade, wenn

$$T^2 - DU^2 = +1,$$

ungerade, wenn

$$T^2 - DU^2 = -1$$

(vorausgesetzt eben, dass dies letztere möglich, d. h. dass die Periodengliederanzahl ungerade sei).

Dann ist

$$\pm 1 = T^2 - DU^2 = \pm \frac{(EE_1)(E_1E_2)\cdots(E_{\mu-1}E_\mu)}{E^2E_1{}^2\cdots E_\mu{}^2}$$

$$= \frac{(\varepsilon^2 - D)(\varepsilon_1{}^2 - D)\cdots(\varepsilon_{\mu-1}{}^2 - D)}{E^2E_1{}^2\cdots E_\mu{}^2}.$$

oder

$$(T + U\sqrt{D})(T - U\sqrt{D})$$

$$= \left\{\frac{(\varepsilon+\sqrt{D})(\varepsilon_1+\sqrt{D})\cdots(\varepsilon_{\mu-1}+\sqrt{D})(\varepsilon-\sqrt{D})(\varepsilon_1-\sqrt{D})\cdots(\varepsilon_{\mu-1}-\sqrt{D})}{EE_1\cdots E_{\mu-1}\,EE_1\cdots E_{\mu-1}}\right\}.$$

Vermöge der hierin vorkommenden $\sqrt{D}$ ist es nun gestattet,

$$T + U\sqrt{D} = \frac{(\varepsilon + \sqrt{D})(\varepsilon_1 + \sqrt{D}) \cdots (\varepsilon_{\mu-1} + \sqrt{D})}{EE_1 \cdots E_{\mu-1}},$$

$$T - U\sqrt{D} = \frac{(\varepsilon - \sqrt{D})(\varepsilon_1 - \sqrt{D}) \cdots (\varepsilon_{\mu-1} - \sqrt{D})}{EE_1 \cdots E_{\mu-1}}$$

zu setzen und, da der rationale Teil sowohl wie der Koeffizient von $\sqrt{D}$ in den Ausdrücken rechts gemäss der Voraussetzung, T und U seien ganze Zahlen, gleichfalls ganzzahlig wird, nun umgekehrt eine der beiden letzten Gleichungen zur Berechnung von T und U zu benutzen.

Lagrange hielt grosse Stücke von der Abhandlung, die wir soeben besprachen. Er äussert sich in diesem Sinne gegen d'Alembert[1]:

„Le problème dont je vous ai parlé[2] m'a occupé beaucoup plus que je ne le pensais d'abord; enfin j'en suis venu heureusement à bout, et je crois n'avoir presque rien laissé à désirer sur le sujet des équations du second degré à deux inconnues"

und indem er d'Alembert zugleich mit dieser Abhandlung den Aufsatz „Sur la résolution des équations numériques"[3]) übersandte, schrieb er[4]:

„Ce sont deux sujets élémentaires, comme vous voyez, mais je puis vous assurer qu'ils m'ont donné plus de peine que toutes mes autres recherches".

Doch lasen weder d'Alembert noch Euler seine Abhandlungen. Ersterer entschuldigte sich mit Krankheit. Der letztere schrieb in dem Briefe, den wir bereits bei früherer Gelegenheit citiert haben[5], dass seine Blindheit ihm nicht gestatte, so komplizierten Darlegungen zu folgen.

Man merkt Lagrange wohl die Enttäuschung an, wenn er in einem aus Anlass des Artikels „Indeterminées" in der Encyklopädie an Condorcet gerichteten Briefe sagt:[6]

„.... quant à [les deux mémoires] ... je vous suis d'autant plus

1) Lagrange an d'Alembert. 23. Févr. 1769. Lagrange Oeuvres. Tome XIII. p. 127.

2) Schon in einem Briefe vom 6. Dez. 1768. Lagrange Oeuvres. Tome XIII. p. 123.

3) „Sur la résolution des équations numériques". Lu à l'Académie de Berlin le 20. avril 1769. Mémoires de l'Académie roy. des sc. et Bell.-L. de Berlin. Tome XXIII. 1769. Oeuvres. Tome II. Paris 1868. p. 539.

4) Lagrange an d'Alembert. 2. Juin 1769. Oeuvres. Tome XIII.

5) Seite 57.

6) Lagrange an Condorcet. 30. Sept. 1771. Oeuvres. Tome XIV.

obligé d'avoir pris la peine, de les lire, que je vous crois le seul, qui m'ait fait cet honneur, car M. Euler qui s'est beaucoup occupé autrefois de ce sujet et qui en a fait longtemps ses délices m'a mandé, que la perte de sa vue ne lui ayant pas permis de lire mes mémoires il n'avait cependant pas manqué de se les faire lire, mais qu'il lui avait été impossible de suivre mes raisonnements et mes calculs".

Doch musste Lagrange selbst zugeben, dass seine Methode komplizierter sei, als wünschenswert. Er sagt: [1])

„La méthode pour le cas où D est un nombre positiv et où p et q [dans l'équation $A = p^2 - Dq^2$] doivent être des nombres entiers, laquelle fait l'objet du § III [du mémoire: „Sur la solution" etc.] est à la vérité un peu longue et compliquée, et j'avoue même qu'elle l'est à un point qui la rend difficile à suivre; mais je crois, que cette difficulté ne doit être imputée qu'à la nature de la matière et au grand nombre de cas aux quels il faut avoir égard, quand on veut la traiter d'une manière aussi directe et aussi rigoureuse que nous l'avons fait. Cepedant j'ai trouvé moyen depuis de simplifier beaucoup cette méthode et de l'étendre même à des équations d'un degré quelconque; c'est ce que je me propose de développer dans ce mémoire avec le plus d'ordre et de clarté qu'il me sera possible".

Das Mittel, worauf Lagrange anspielt, ist eine andere Reduktion der Aufgabe und eine ausgedehnte Anwendung der Kettenbrüche.

Wir sahen bereits, dass die Methode, welche Lagrange in der letztbesprochenen Abhandlung zur Lösung der Gleichung $A = t^2 - Du^2$ anwandte, im Grunde auf der Entwicklung von $\sqrt{D}$ in einen Kettenbruch beruhte.

Auf diese Seite der Sache war Lagrange in anderem Zusammenhange, vielleicht zum Teil auch durch die Eulersche Abhandlung „De usu novi algorithmi" aufmerksam geworden, die er inzwischen kennen gelernt hatte.

Infolge der Abhandlung „Sur la résolution des équations numériques [2]), deren Methode darauf beruht, eine zu berechnende reelle positive Wurzel,

---

1) Nouvelle méthode pour résoudre les problèmes indéterminés en nombres entiers. Lu à l'Académie le 21. Juin 1770. Mém. Tome XXIV. Oeuvres. Tome II. Paris 1867. p. 658.

2) „Sur la résolution des équations numériques". Lu à l'Académie de Berlin le 20. avril 1769. Mémoire de l'Académie roy. des sc. et Bell.-L. de Berlin. Tome XXIII. 1769. Oeuvres. Tome II. Paris 1868. p. 539.

wenn man sie zwischen zwei ganze Zahlen eingeschlossen hat, durch die Substitutionen

$$x = \lambda_1 + \frac{1}{x_1} \{x_1 > 1,\ \lambda_1 = \text{num. integ.}\},$$

$$x_1 = \lambda_2 + \frac{1}{x_2} \text{ etc.}$$

in einen Kettenbruch zu verwandeln, unterzog Lagrange die quadratischen Gleichungen mit nur reellen irrationalen Wurzeln, also mit positiver nicht quadratischer Determinante einer genauen Untersuchung in Bezug auf die Kettenbruchentwicklung ihrer Wurzeln.

Dann wird in den „Additions au Mémoire sur la résolution des équations numériques [1])“ durch Betrachtung der durch die Substitutionen $x_\nu = \lambda_{\nu+1} + \frac{1}{x_{\nu+1}}$ transformierten Gleichungen gezeigt, dass dieselben von einem gewissen Punkte ab „reduzierte“ werden und sich ebenso wie die Grössen λ und x periodisch wiederholen, die Kettenbruchentwicklung also von einer gewissen Stelle ab periodisch wird.

Die hier gewonnenen Resultate werden nun von Lagrange in der [2]) Abhandlung „Nouvelle méthode pour résoudre les problèmes indetérminés en nombres entiers“ zur Vereinfachung der Theorie der Darstellung einer Zahl durch eine binäre quadratische Form von positiver Determinante benutzt.

Er geht aus von sehr allgemeinen Betrachtungen.

Die Lösung der Gleichung

$$A = Bt^n + \Gamma t^{n-1}u + \Delta t^{n-2}u^2 \text{ etc.} + Ku^n,$$

wird zurückgeführt auf die einer Gleichung

$$1 = Pu^n + Qu^{n-1}y + \ldots + Vy^n = \Phi.$$

Diese Aufgabe wird darauf reduziert, alle positiven reellen Wurzeln der Gleichung

$$Px^n + Qx^{n-1} + \ldots + V = 0 = z,$$

in Kettenbrüche zu entwickeln und die Näherungsbrüche derselben in

1) Lu à l'Académie le 25. août 1769 et le 8. mars 1770. Mémoires de l'Académie roy. d. Sc. et B.-L. de Berlin. Tome XXIV. 1770. § II. Oeuvres de Lagrange. Tome II. p. 593 u. f.

2) Lu à l'Académie le 21. Juin 1770. Mém. Tome XXIV. Oeuvres. Tome II. p. 655 u. f.

die Gleichung Φ einzusetzen oder, was auf dasselbe herauskommt, zuzusehen, ob unter den vermöge der Substitutionen

$$x = \lambda_1 + \frac{1}{x_1};\ x_1 = \lambda_2 + \frac{1}{x_2} \text{ etc.}$$

transformierten Gleichungen

$$z = 0;\ z_1 = 0;\ z_2 = 0 \ldots \text{ bis } z_\varrho = 0 \text{ etc.}$$

sich eine befindet, deren erstes Glied den Koeffizienten[1]) 1 hat. Ist dies der Fall, so löst der zu der betreffenden Stelle der Kettenbruchentwicklung gehörige Näherungsbruch die Gleichung $\Phi = 1$, wenn man seinen Zähler an Stelle von u, seinen Nenner an Stelle von y in Φ einsetzt.

Nun wird aber im Falle einer quadratischen Gleichung mit positiver Determinante

$$P\mu^2 + Q\mu y + Ry^2 = 1,$$

die Gleichung

$$Px^2 + Qx + R = 0,$$

von deren Wurzeln das Verfahren abhängt auf die Form

$$\varphi_1 = E_1 x^2 - 2\varepsilon x - E = 0$$

gebracht und eine ihrer positiv genommenen Wurzeln in einen Kettenbruch entwickelt. Nach dem erwähnten Satze wird dieser sowie die Folge der transformierten Gleichungen $\varphi_2 = 0 \ldots \varphi_\varrho = 0$ von einer Stelle ab periodisch und zwar von der Stelle, wo zwei aufeinanderfolgende E gleiches Vorzeichen haben. Eins von beiden wird dann $< \sqrt{D}$ sein und schon mit zur Periode gehören. Findet sich in der Reihe der E ein Glied, welches gleich der Einheit, so ist die vorgelegte Gleichung durch den zu dieser Stelle gehörigen Näherungsbruch lösbar. Daraus folgt, wie Lagrange zeigt, dass jede Gleichung

$$E_1 = E_1\mu^2 - 2\varepsilon\mu y - Ey^2$$

durch beliebig viele Paare ganzer Zahlen befriedigt werden kann.

Die Fermatsche Gleichung $t^2 - Du^2 = 1$ ist nun aber ein Spezialfall der letztgenannten, in welchem $E_1 = 1$, $\varepsilon = 0$, $E = D$. Man kann sie somit auflösen, indem man eine positive Wurzel der Gleichung

1) Dieser Koeffizient ist eben $\Phi(p_\varrho, q_\varrho)$, wenn $\frac{p_\varrho}{q_\varrho}$ der ϱte Näherungsbruch.

$x^2 - D = 0$, d. h. $\sqrt{D}$ in einen Kettenbruch entwickelt; da $E_1 = E_2 = 1$, also $E_1 < \sqrt{D}$, beginnt die Periode mit der Einheit; je nachdem die Gliederzahl der Periode gerade oder ungerade ist, wird man am Schlusse jeder oder am Schlusse jeder zweiten Periode der E die Einheit wieder finden und somit mit Zähler und Nenner des zugehörigen Näherungsbruches die Gleichung $t^2 - Du^2 = 1$ lösen können.

Lagrange hat das soeben besprochene Verfahren und seinen Beweis nochmals von einem fast gleichen Standpunkte aus in den „Additions aux élémens d'algèbre d'Euler"[1]), entwickelt.

Auch hier gilt die Fermatsche Gleichung als spezieller Fall des allgemeineren Problems der Darstellung einer Zahl durch eine quadratische Form von positiver Determinante.

Zunächst wird die allgemeinere Gleichung auf die spezielle

$$\Phi = Py^2 - 2Qyz + Rz^2 = 1$$

zurückgeführt, wo $P < \sqrt{D}$

$$|2Q| < P,$$
$$D = Q^2 - PR > 0.$$

Infolge dieser letzten Bedingung ist 1 das Minimum der Formel für ganzzahlige y und z.

Lagrange untersucht nun ganz allgemein die Frage nach der Bestimmung des auf ganzzahlige Werte der Veränderlichen bezüglichen Minimums einer homogenen binären Form $n$ten Grades, indem er diese in Faktoren zerlegt denkt. Er zeigt, dass die Zahlen, welche diese Form zu einem Minimum machen, sich unter denjenigen Zahlen p, q befinden, durch welche der Ausdruck $p - \alpha q$ kleiner wird, als durch irgend zwei kleinere Zahlen p_1, q_1, wenn α eine beliebige positive reelle Wurzel der Gleichung bedeutet, welche man erhält, indem man die homogene Funktion $\Phi_1(t, u) = 0$ setzt, durch u^n dividiert und $\frac{t}{u}$ als neue Variable wählt, und von welcher wir der Einfachheit halber hier voraussetzen, dass sie nur positive oder negative, reelle und irrationale Wurzeln habe, wie es bei den homogenen quadratischen Formen mit positiver Determinante ja der Fall ist. Die weitere Untersuchung ergiebt dann, dass jedes durch die obige Bedingung geforderte Zahlenpaar p, q die Eigenschaft hat, einen

1) Siehe Seite 57.

Näherungsbruch $\frac{p}{q}$ für die irrationale Grösse α zu liefern. Man hat also die Näherungsbrüche für die verschiedenen Wurzeln von Φ_1 zu bilden und Zähler und Nenner derselben resp. an Stelle von t und u einzusetzen, um zu sehen, wann Φ_1 den kleinsten Wert erhält.

Nun wird, wie Lagrange zeigt, die Kettenbruchentwicklung der Wurzeln der zugehörigen Gleichung im Falle quadratischer binärer homogener Formen mit positiver Determinante periodisch. Die Nenner der Brüche, durch welche die Teilnenner der Kettenbruchentwicklung bestimmt werden, sind nichts anderes als die ursprüngliche Form Φ, in welche Zähler und Nenner des zu der betreffenden Stelle gehörigen Näherungsbruches statt y und x eingesetzt wurden. Man hat also nur zuzusehen, ob im Laufe einer Periode einer dieser Nenner resp. ein äusserer Koeffizient der durch die Substitutionen $x_\nu = \lambda_{\nu+1} + \frac{1}{x_{\nu+1}}$ etc. transformierten Gleichungsfolge gleich der Einheit wird, um zu wissen, ob die vorgelegte Gleichung eine Lösung zulässt oder nicht.

Da nun in unserem Falle die Periodizität des Kettenbruches gleich mit dem ersten Glied beginnt, und der hierzu gehörige Wert $\Phi(1,0) = 1$, so muss dieser zum mindesten bei jeder zweiten Periode wiederkehren, und der zugehörige Näherungsbruch für $\sqrt{D}$ also jedes mal eine Lösung der Gleichung $t^2 - Du^2 = 1$ liefern.

Das ist in aller Kürze Lagranges letzte Untersuchung und Darstellung unseres Gegenstandes, von der er selbst meint „qu'elle était tirée des vrais principes de la chose et ne laissait rien à désirer".[1])

Es bleibt noch übrig anzuführen, dass aus dieser Methode, wie Lagrange zeigt, sich auch das Wallis-Brounckersche Verfahren ableiten und als richtig beweisen lässt.

Nehmen wir an, es sei

$$p^2 - Dq^2 = 1,$$

dann ist, wie wir sahen, $\frac{p}{q}$ ein Näherungsbruch der Kettenbruchentwicklung für $\sqrt{D}$; entwickelt man also nun seinerseits $\frac{p}{q}$ in einen Kettenbruch, so muss man sämtliche Teilnenner gerade so erhalten, wie bei der Entwicklung von $\sqrt{D}$ bis zu der Stelle, welcher $\frac{p}{q}$ entspricht.

1) Additions Art. 84. Oeuvres. Bd. VII. p. 159, l. 2.

Bestimmt man also aus der Gleichung

$$p^2 - Dq^2 = 0\,,\; p = \mu q + r,\; r < q,$$

sodann aus der Gleichung der transformierten Form

$$(\mu^2 - D)\left(\frac{q}{r}\right)^2 + 2\mu\left(\frac{q}{r}\right) + 1 = 0,$$

$$q = \mu_1 r + s \text{ etc.},$$

so werden die Zahlen μ_k mit den Teilnennern der Kettenbruchentwicklung von $\sqrt{D}$ identisch sein, und man muss also an jedem Perioden- resp. Doppelperiodenschluss zu einer transformierten Form gelangen, deren erster Koeffizient gleich der Einheit ist, und die somit die Eins darstellt, wenn man der ersten Veränderlichen den Wert 1, der zweiten den Wert 0 beilegt. Die unterwegs ermittelten Zahlen $\mu_1 \ldots \mu_k$ gestatten dann von dem fingierten Näherungsbruch $\frac{1}{0}$ zu $\frac{p}{q}$ selbst zurückzusteigen.

Nun ändert sich aber offenbar an dem ganzen Verfahren nichts, wenn man mit Wallis statt die Gleichung $p^2 - Dq^2 = 0$ zu wählen, und so stets homogene transformierte Formen zu erhalten, von der Gleichung $t^2 - Du^2 = 1$ zur Bestimmung von $\frac{p}{q}$ ausgeht. Man braucht sich dann, wie es in der That bei dem Wallisschen Verfahren geschieht, bei der Bestimmung des Koeffizienten μ_k gar nicht um das mit dem konstanten Term und der — 2. Potenz der zweiten Unbekannten behaftete Glied zu kümmern, um sicher zu sein, dass man beliebig oft zu einer Gleichung gelangen wird, welche durch die Annahme: erste Unbekannte = 1, zweite Unbekannte = 0 befriedigt wird und somit als Fusspunkt zur Berechnung einer Lösung dienen kann.

Wie wir sehen, kommt die letzte von Lagrange angegebene Methode in dem speziellen Falle der Fermatschen Gleichung auf das Eulersche Verfahren vom Jahre 1765 heraus. Legendre hat dem Beweise Lagranges gerade für unsere Aufgabe eine besonders einfache Form gegeben[1]) und da es des Zusammenhangs und der Allgemeinheit von Lagranges Betrachtungen wegen nicht möglich war, alles zu dem strengen Beweise nötige Detail hier wiederzugeben, füge ich, als Abschluss und Zusammenfassung der auf der Benutzung von Kettenbrüchen mit

1) A. M. Legendre, Théorie des nombres. Troisième édition. Tome I. Paris 1830. p. 51 u. f.

positiven Teilnennern beruhenden Methoden Beweis und Verfahren nach Legendre bei.

Wir setzen voraus, dass folgende drei Lehrsätze von den Kettenbrüchen mit den Teilzählern 1 und positiven Teilnennern bewiesen seien.

Hilfssatz I.

Sind

$$\frac{p_\varrho}{q_\varrho}, \quad \frac{p_{\varrho+1}}{q_{\varrho+1}} = \frac{p_\varrho \mu_\varrho + p_{\varrho-1}}{q_\varrho \mu_\varrho + q_{\varrho-1}}$$

zwei aufeinanderfolgende Näherungsbrüche des Kettenbruches

$$K = \mu + \frac{1}{\mu_1 + \frac{1}{\mu_2 + \dots}},$$

so ist

$$p_{\varrho+1} q_\varrho - p_\varrho q_{\varrho+1} = (-1)^{\varrho+1}.$$

Hilfssatz II.

Ist $\frac{p_\varrho}{q_\varrho}$ der ϱte Näherungsbruch des nämlichen Kettenbruches K und z_ϱ der zur Stelle ϱ gehörige vollständige Quotient, so ist

$$K = \frac{p_\varrho z_\varrho + p_{\varrho-1}}{q_\varrho z + q_{\varrho-1}}.$$

Hilfssatz III.

Bezeichnen $\frac{p_\varrho}{q_\varrho}, \frac{p_{\varrho+1}}{q_{\varrho+1}}$ den vorletzten und letzten Näherungsbruch des endlichen Kettenbruches

$$\frac{1}{\mu_1 + \frac{1}{\mu_2 + \dots + \frac{1}{\mu_{\varrho+1}}}}$$

und ist

$$q_\varrho = p_{\varrho+1},$$

so wird

$$\mu_{(\varrho+1)-k} = \mu_{(1)+k}.$$

I. Entwickelt man $\sqrt{D}$, $D = a^2 + b$, $o < b < a$, in einen Kettenbruch

$$a + 1$$
$$\mu_1 + 1$$
$$\mu_2 + \text{etc.},$$

so haben alle vollständigen Quotienten x_ϱ die Form $\frac{\sqrt{D} + \varepsilon_\varrho}{E_\varrho}$, wo E_ϱ und ε_ϱ ganze Zahlen, und man findet aus x_ϱ, $x_{\varrho+1}$, indem man setzt

$$\varepsilon_{\varrho+1} = \mu_\varrho E_\varrho - \varepsilon_\varrho,$$

$$E_{\varrho+1} = \frac{D - \varepsilon_{\varrho+1}^2}{E_\varrho} = E_{\varrho-1} + \mu_\varrho(\varepsilon_\varrho - \varepsilon_{\varrho+1}).$$

Beweis. Wir nehmen an, unsere Behauptung sei schon bewiesen bis zu dem vollständigen Quotiente x_ϱ, dann ist (μ_ϱ die grösste ganze Zahl in x_ϱ),

$$x_\varrho = \frac{\sqrt{D} + \varepsilon_\varrho}{E_\varrho} = \mu_\varrho + \frac{1}{x_{\varrho+1}},$$

also

$$x_{\varrho+1} = \frac{E_\varrho}{\sqrt{D} + \varepsilon_\varrho - \mu_\varrho E_\varrho}$$
$$= \frac{E_\varrho(\sqrt{D} - (\varepsilon_\varrho - \mu_\varrho E_\varrho))}{D - (\varepsilon_\varrho - \mu_\varrho E_\varrho)^2};$$

setzen wir

$$\mu_\varrho E_\varrho - \varepsilon_\varrho = \varepsilon_{\varrho+1}, \quad \frac{D - \varepsilon_{\varrho+1}^2}{E_\varrho} = E_{\varrho+1},$$

so muss noch gezeigt werden, dass $E_{\varrho+1}$ ganzzahlig wird, alsdann ist

$$x_{\varrho+1} = \frac{\sqrt{D} + \varepsilon_{\varrho+1}}{E_{\varrho+1}}.$$

$E_{\varrho+1}$ ist aber ganzzahlig, denn man hat

$$E_{\varrho+1} = \frac{D - (\mu_\varrho E_\varrho - \varepsilon_\varrho)^2}{E_\varrho} = \frac{D - \varepsilon_\varrho^2}{E_\varrho} + 2\mu_\varrho\varepsilon_\varrho - \mu_\varrho^2 E_\varrho.$$

Da wir annahmen, unser Satz sei bis zum vollständigen Teilnenner x_ϱ bewiesen, folgt

$$\frac{D - \varepsilon_\varrho^2}{E_{\varrho-1}} = E_\varrho, \text{ also } D - \varepsilon_\varrho^2 = E_\varrho E_{\varrho-1},$$

somit

$$E_{\varrho+1} = E_{\varrho-1} + 2\mu_\varrho\varepsilon_\varrho - \mu_\varrho^2 E_\varrho$$
$$= E_{\varrho-1} + \mu(\varepsilon_\varrho - \varepsilon_{\varrho+1}) = \text{num. integ.}$$

Nun ist aber für die beiden ersten Teilnenner das angegebene Gesetz jedenfalls gültig, da

$$\sqrt{D} = a + \frac{1}{x_1} = a + \frac{\sqrt{D} - a}{1},$$

$$x_1 = \frac{\sqrt{D} + a}{D - a^2} = \frac{\sqrt{D} + a}{\mathfrak{b}},$$

also

$$x = \frac{\sqrt{D} + 0}{1}, \quad x_1 = \frac{\sqrt{D} + a}{\mathfrak{b}}.$$

Daraus folgt, wie gezeigt, dass es auch für $x_2, x_3 \ldots x_n, x_{n+1}$ gilt.

q. e. d.

II. Sind wie eben $\frac{p_{\varrho-1}}{q_{\varrho-1}}, \frac{p_\varrho}{q_\varrho}$ zwei aufeinanderfolgende Näherungsbrüche für $\sqrt{D}$ und haben die Zeichen: x_ϱ, E_ϱ, ε_ϱ die gleiche Bedeutung, so ist

$$(1) \qquad (-1)^\varrho E_\varrho = p_\varrho^2 - Dq_\varrho^2,$$

$$(2) \qquad (-1)^\varrho E_\varrho = q_\varrho q_{\varrho-1} D - p_\varrho p_{\varrho-1}$$

wo E_ϱ, ε_ϱ stets positive Zahlen.

Beweis. Nach Hilfssatz II ist

$$\sqrt{D} = \frac{p_\varrho x_\varrho + p_{\varrho-1}}{q_\varrho x_\varrho + q_{\varrho-1}} = \frac{p_\varrho\sqrt{D} + p_\varrho\varepsilon_\varrho + p_{\varrho-1}E_\varrho}{q_\varrho\sqrt{D} + q_\varrho\varepsilon_\varrho + q_{\varrho-1}E_\varrho}.$$

Durch Trennung des rationalen und des irrationalen Bestandteiles folgt hieraus

$$p_\varrho\varepsilon_\varrho + p_{\varrho-1}E_\varrho = q_\varrho D,$$
$$q_\varrho\varepsilon_\varrho + q_{\varrho-1}E_\varrho = p_\varrho$$

und aus diesen Gleichungen:

$$(p_\varrho q_{\varrho-1} - q_\varrho p_{\varrho-1})\varepsilon_\varrho = q_\varrho Q_{\varrho-1} D - p_\varrho p_{\varrho-1},$$
$$(p_\varrho q_{\varrho-1} - q_\varrho p_{\varrho-1})E_\varrho = p_\varrho^2 - Dq_\varrho^2,$$

oder nach Hilfssatz I

$$(-1)^\varrho\varepsilon_\varrho = q_\varrho q_{\varrho-1} D - p_\varrho p_{\varrho-1},$$
$$(-1)^\varrho E_\varrho = p_\varrho^2 - Dq_\varrho^2.$$

Es bleibt nur noch zu zeigen, dass ε_ϱ und E_ϱ beide positiv. Nun aber ist

$$\frac{p_\varrho}{q_\varrho} > \sqrt{D}, \text{ wenn } \varrho = 2n,$$

$$\frac{p_\varrho}{q_\varrho} < \sqrt{D}, \quad \text{,,} \quad \varrho = 2n+1;$$

beide Seiten der Gleichung

$$(-1)^\varrho \frac{E_\varrho}{(q_\varrho)^2} = \left(\frac{p_\varrho}{q_\varrho}\right)^2 - D$$

haben somit stets gleiches Vorzeichen. Also muss E_ϱ positiv sein.

Zweitens ist

$$q_\varrho \varepsilon_\varrho + q_{\varrho-1} E_\varrho = p_\varrho,$$

also

$$\frac{q_{\varrho-1}}{q_\varrho} = \frac{\left(\frac{p_\varrho}{q_\varrho} - \varepsilon_\varrho\right)}{E_\varrho}$$

und da vermöge

$$q_{\varrho-1} = \frac{q_\varrho - q_{\varrho-2}}{\mu_\varrho}, \quad q_{\varrho-1} < q_\varrho,$$

wird

$$E_\varrho > \frac{p_\varrho}{q_\varrho} - \varepsilon_\varrho,$$

also, da $\sqrt{D}$ irrational, E_ϱ positiv und ε_ϱ ganzzahlig, endlich $\frac{p_\varrho}{q_\varrho}$ ein Näherungsbruch zu $\sqrt{D}$,

$$E_\varrho > \sqrt{D} - \varepsilon_\varrho.$$

Ferner ist

$$\frac{\sqrt{D} + \varepsilon_\varrho}{E_\varrho} = x_\varrho = \mu_\varrho + \frac{1}{x_{\varrho+1}},$$

also da

$$\mu_\varrho \geqq 1,$$

$$E_\varrho < \sqrt{D} + \varepsilon_\varrho.$$

Diese beiden Ungleichungen würden sich aber widersprechen, wenn $\varepsilon_\varrho < 0$ wäre. Es sind somit sämtliche E und ε positive Zahlen.

III. Die Kettenbruchentwicklung für $\sqrt{D}$ ist periodisch. Die Perioden beginnen hinter dem ersten Glied des Kettenbruches a; sie sind symmetrisch und von einander jedesmal durch einen Teilnenner $2a$ getrennt.

A. Die Kettenbruchentwicklung für $\sqrt{D}$ wird periodisch.

Beweis. Da

$$D - \varepsilon_\varrho^2 = E_\varrho E_{\varrho-1}$$

und alle ε und E positiv, folgt allgemein

$$E_\varrho < D, \qquad \varepsilon_\varrho < \sqrt{D}$$

oder da ε_ϱ eine ganze Zahl

$$\varepsilon_\varrho \leq a.$$

Ferner weil

$$\varepsilon_{\varrho+1} = \mu_\varrho E_\varrho - \varepsilon_\varrho,$$

$$\mu_\varrho E_\varrho = \varepsilon_{\varrho+1} + \varepsilon_\varrho,$$

$$\varepsilon_{\varrho+1} \leq a, \qquad \varepsilon_\varrho \leq a,$$

also

$$\mu_\varrho E_\varrho \leq 2a$$

und

$$\mu_\varrho \leq 2a, \qquad E_\varrho \leq 2a.$$

Es giebt also nur eine begrenzte Zahl Werte, welche E_ϱ, ε_ϱ, μ_ϱ erhalten können. Da aber $\sqrt{D}$ irrational, kann man den Kettenbruch für $\sqrt{D}$ beliebig weit fortsetzen. Es muss also der Fall eintreten, dass einmal eine Kombination von E und ε, also ein vollständiger Quotient $\frac{\sqrt{D} + \varepsilon_\varrho}{\varepsilon_\varrho}$ wiederkehrt, welcher schon einmal da war, und da vermöge der Formeln aus I durch x_ϱ alle folgenden $E_{\varrho+\nu}$, $\varepsilon_{\varrho+\nu}$ bestimmt sind, müssen von dieser Stelle ab alle Teilnenner μ sowie die Grössen x, E, ε in der gleichen Reihenfolge wiederkehren, wie sie zum ersten Mal erschienen sind.

B. Die Perioden des Kettenbruches beginnen hinter dem ersten ganzzahligen Gliede a.

Beweis. Nehmen wir an, der Teilnenner μ_ϱ $(\varrho > 1)$ beginne die Periode, so dass $\mu_{\varrho+x\pi} = \mu_\varrho$, wenn x eine beliebige ganze Zahl. Dann ist $E_{\varrho+x\pi} = E_\varrho$; $\varepsilon_{\varrho+x\pi} = \varepsilon_\varrho$.

Also da

$$D - \varepsilon_{\varrho+x\pi}^2 = E_{\varrho+x\pi} E_{\varrho+x\pi-1}$$

oder

$$D - \varepsilon_\varrho^2 = E_\varrho E_{\varrho+x\pi-1}$$

und

$$D - \varepsilon_\varrho^2 = E_\varrho E_{\varrho-1}$$

folgt

$$E_{\varrho-1} = E_{\varrho+x\pi-1}.$$

Ferner ist

$$\varepsilon_\varrho = \mu_{\varrho-1} E_{\varrho-1} - \varepsilon_{\varrho-1},$$

$$\varepsilon_\varrho = \varepsilon_{\varrho+x\pi} = \mu_{\varrho+x\pi-1} E_{\varrho+x\pi-1} - \varepsilon_{\varrho+x\pi-1} = \mu_{\varrho+x\pi-1} E_{\varrho-1} - \varepsilon_{\varrho+x\pi-1},$$

also

$$\frac{E_{\varrho+x\pi-1} - \varepsilon_{\varrho-1}}{E_{\varrho-1}} = \mu_{\varrho+x\pi-1} - \mu_{\varrho-1}.$$

Nun ist aber (II)

$$q_\varrho \varepsilon_\varrho + q_{\varrho-1} E_\varrho = p_\varrho,$$

also

$$\varepsilon_\varrho = \frac{p_\varrho}{q_\varrho} - \frac{q_{\varrho-1}}{q_\varrho} E_\varrho.$$

Da $\frac{p_\varrho}{q_\varrho}$ ein Näherungsbruch für $\sqrt{D}$,

$$\frac{p_\varrho}{q_\varrho} = a + \frac{r}{q} \quad \left(r \lesssim \begin{matrix}1\\0\end{matrix}\right),$$

also

$$a - \varepsilon_\varrho = \frac{q_{\varrho-1} E_\varrho - r}{q_\varrho},$$

wird

$$a - \varepsilon_\varrho < \frac{q_{\varrho-1}}{q_\varrho} E_\varrho,$$

somit, da $q_{\varrho-1} < q_\varrho$, a fortiori

$$a - \varepsilon_\varrho < E_\varrho;$$

gerade so folgt aber aus

$$q_{\varrho+x\pi-1} \varepsilon_{\varrho+x\pi-1} + q_{\varrho+x\pi-2} E_{\varrho-1} = p_{\varrho+x\pi-1},$$

$$a - \varepsilon_{\varrho+x\pi-1} < E_{\varrho-1} \quad (\text{da ja } E_{\varrho-1} = E_{\varrho+x\pi-1})$$

und aus

$$\breve{q}_{\varrho-1} \varepsilon_{\varrho-1} + q_{\varrho-2} E_{\varrho-1} = p_{\varrho-1},$$

$$a - \varepsilon_{\varrho-1} < E_{\varrho-1},$$

also

$$|\varepsilon_{\varrho+x\pi-1} - \varepsilon_{\varrho-1}| < E_{\varrho-1}.$$

Nun war aber

$$\frac{\varepsilon_{\varrho+x\pi-1} - \varepsilon_{\varrho-1}}{E_{\varrho-1}} = \mu_{\varrho+x\pi-1} - \mu_{\varrho-1},$$

es müsste also

$$|\mu_{\varrho+x\pi-1} - \mu_{\varrho-1}| < 1$$

sein; da aber $\mu_{\varrho+x\pi-1}$, ebenso wie $\mu_{\varrho-1}$ ganze Zahlen sind, ist dies nur möglich, wenn

$$\mu_{\varrho+x\pi-1} = \mu_{\varrho-1},$$

also auch

$$\varepsilon_{\varrho+x\pi-1} = \varepsilon_{\varrho-1}.$$

Wir haben also

$$\varkappa_{\varrho+x\pi-1} = \varkappa_{\varrho-1},$$

$$E_{\varrho+x\pi-1} = E_{\varrho-1}; \quad \varepsilon_{\varrho+x\pi-1} = \varepsilon_{\varrho-1}; \quad \mu_{\varrho-1} = \mu_{\varrho+x\pi-1}.$$

Man gelangt somit von dem $\varrho - 1$ten Gliede aus durch die nämlichen Schlüsse wie eben zu dem Nachweis, dass

$$\varkappa_{\varrho+x\pi-2} = \varkappa_{\varrho-2}; \qquad E_{\varrho+x\pi-2} = E_{\varrho-2},$$

$$\varepsilon_{\varrho+x\pi-2} = \varepsilon_{\varrho-2}; \qquad \mu_{\varrho+\pi x-2} = \mu_{\varrho-2}.$$

Es zeigt sich also, dass die Glieder des Kettenbruches vor der ϱten Stelle der Grösse und Ordnung nach mit denen der Periode übereinstimmen. Sie müssen aber auch eine vollständige Periode bilden, denn wäre μ_1 nicht gleich μ_ϱ $(\varrho = \pi + 1)$, so könnte entgegen der Voraussetzung μ_ϱ nicht der erste Teilnenner sein, der wiederkehrt.

Die erste Periode beginnt also sogleich mit μ_1.

C. Alle Perioden schliessen mit dem Teilnenner $2a$; von diesem abgesehen ist die Periode symmetrisch.

Beweis. Es sei $\mu_{x\pi}$ der letzte Teilnenner der $x$ten Periode, $\varkappa_{x\pi}$ der zugehörige vollständige Quotient. Dann ist

$$\varkappa_{x\pi} = \mu_{x\pi} + \frac{1}{\varkappa_{x\pi+1}} = \mu_{x\pi} + \frac{1}{\varkappa_1} = \mu_{x\pi} + \frac{1}{\frac{\sqrt{D}+a}{b}} = \mu_{x\pi} + \sqrt{D} - a$$

und nach Hilfssatz II

$$\sqrt{D} = \frac{p_{x\pi}\varkappa_{x\pi} + p_{x\pi-1}}{q_{x\pi}\varkappa_{x\pi} + q_{x\pi-1}} = \frac{p_{x\pi}(\mu_{x\pi} + \sqrt{D} - a) + p_{x\pi-1}}{q_{x\pi}(\mu_{x\pi} + \sqrt{D} - a) + q_{x\pi-1}}.$$

Das giebt nach Trennung des rationalen und irrationalen Bestandteils

$$p_{x\pi}(\mu_{x\pi} - a) + p_{x\pi-1} = Dq_{x\pi},$$

$$q_{x\pi}(\mu_{x\pi} - a) + q_{x\pi-1} = p_{x\pi}.$$

Die zweite dieser Gleichungen liefert

$$\mu_{x\pi} - a + \frac{q_{x\pi-1}}{q_{x\pi}} = \frac{p_{x\pi}}{q_{x\pi}}$$

und da $q_{x\pi-1} < q_{x\pi}$, ist hieraus zu schliessen, dass $\mu_{x\pi} - a$ die grösste ganze in $\frac{p_{x\pi}}{q_{x\pi}}$ enthaltene ganze Zahl bedeutet. Diese grösste ganze Zahl ist aber a, da $\frac{p_{x\pi}}{q_{x\pi}}$ ein Näherungsbruch zu $\sqrt{D}$. Somit kommt

$$\mu_{x\pi} - a = a,$$

also wie behauptet

$$\mu_{x\pi} = 2a.$$

Betrachten wir nun

$$\frac{p_\pi}{q_\pi} - a,$$

so ist dies gleich dem bis zum Schluss der ersten Periode fortgesetzten Kettenbruche für $\sqrt{D}$, jedoch ohne das ganzzahlige Glied a und ohne den letzten Teilnenner 2μ

$$\frac{p_\pi - aq_\pi}{q_\pi} = \cfrac{1}{\mu_1 + \cfrac{1}{\mu_2 + \cdots + \cfrac{1}{\mu_{\pi-1}}}}.$$

Die letzte Gleichung der vorigen Seite liefert aber:

$$aq_\pi + q_{\pi-1} = p_\pi$$

oder

$$q_{\pi-1} = p_\pi - aq_\pi.$$

Nun ist ferner

$$\frac{p_{\pi-1}}{q_{\pi-1}} - a$$

oder

$$\frac{p_{\pi-1} - aq_{\pi-1}}{q_{\pi-1}}$$

der zweitletzte Näherungsbruch für die bis zum ersten Teilnenner $2a$ excl. fortgesetzte Kettenbruchentwicklung für $\sqrt{D} - a$, so dass

$$\frac{p_{\pi-1} - aq_{\pi-1}}{q_{\pi-1}} = \frac{p_{\pi-1} - aq_{\pi-1}}{p_\pi - aq_\pi}$$

und

$$\frac{p_\pi - a q_\pi}{q_\pi}$$

die beiden letzten Näherungsbrüche für

$$\cfrac{1}{\mu_1 + \cfrac{1}{\mu_2 + \cfrac{1}{\mu_3 + \cdots \cfrac{}{\cdots \frac{1}{\mu_{\pi-1}}}}}} \quad \text{sind.}$$

Da der Nenner des vorletzten Bruches gleich dem Zähler des letzten ist, wird also nach Hilfssatz II

$$\mu_{k+1} = \mu_{\pi-1-k} \quad (k \leq \pi - 2).$$

Die erste Periode (abgesehen von $2a$) ist somit symmetrisch und daher sämtliche Perioden.

IV. Die Gleichung $t^2 - Du^2 = 1$ ist stets ganzzahlig lösbar und zwar durch Zähler und Nenner jedes zu einem Teilnenner $2a$ gehörigen Näherungsbruches der Kettenbruchentwicklung von $\sqrt{D}$, wenn die Periode

$$\mu_1;\ \mu_2 \cdots \mu_2;\ \mu_1$$

ein mittleres Glied hat; durch Zähler und Nenner des zu jedem 2ten Teilnenner $2a$ gehörigen Näherungsbruches, wenn die Periode

$$\mu_1;\ \mu_2 \cdots \mu_2;\ \mu_1$$

kein mittleres Glied besitzt.

Beweis. Unter Nr. II wurde gezeigt, dass stets

$$(-1)^\varrho E_\varrho = p_\varrho^2 - D q_\varrho^2,$$

wenn $\frac{p_\varrho}{q_\varrho}$ der zum Teilnenner μ_ϱ gehörige (d. h. durch Abbrechen vor demselben) entstandene Näherungsbruch ist. Ferner war (S. 94)

$$E_\varrho \mu_\varrho = \varepsilon_\varrho + \varepsilon_{\varrho-1}$$

und $\varepsilon < a$. Da hier $\mu_\varrho = 2a$, muss offenbar

$$\varepsilon_\varrho = \varepsilon_{\varrho-1} = a$$

und

$$E_\varrho = 1$$

sein. Also hat man

$$(-1)^\varrho = p_\varrho^2 - Dq_\varrho^2.$$

Soll

$$p_\varrho^2 - Dq_\varrho^2 = 1,$$

also ϱ gerade sein, so muss entweder die Anzahl der Periodenstellen π gerade und $\varrho = x\pi$ sein; dann hat der symmetrische Teil der Periode $\pi - 1$ Glieder, also ein mittleres. Oder die Zahl der Periodenglieder ist ungerade. Dann wird $\pi - 1$ ungerade, der symmetrische Teil der Periode hat kein Mittelglied, und man muss $\varrho = 2x\pi$ nehmen. q. e. d.

V. **Man erhält** nach dem angegebenen Verfahren alle möglichen Lösungen der Gleichung $t^2 - Du^2 = 1$. Diejenige, welche man am Schlusse der ersten Periode der Kettenbruchentwicklung für $\sqrt{D}$ bekommt, ist abgesehen vom Vorzeichen die kleinste.

Beweis. 1. ede Lösung p'_ϱ, q'_ϱ der Gleichung $p'^2_\varrho - q'^2_\varrho D = 1$ liefert einen Näherungsbruch der Kettenbruchentwicklung für $\sqrt{D}$.

Wir stützen uns auf folgendes Lemma, das wir als bewiesen voraussetzen.

Ist der Bruch $\frac{p_\varrho}{q_\varrho}$ gegeben und ist seine Differenz mit einer zweiten Grösse x gleich

$$\frac{\pm d}{q_\varrho^2}, \quad |d| < 1,$$

so ist $\frac{p_\varrho}{q_\varrho}$ ein Näherungsbruch der Kettenbruchentwicklung für x, wenn

$$d < \frac{q_\varrho}{q_\varrho + q_{\varrho-1}},$$

wo $q_{\varrho-1}$ den Nenner desjenigen Näherungsbruches für x bedeutet, welcher $\frac{p_\varrho}{q_\varrho}$ unmittelbar vorausgeht, wenn man $\frac{p_\varrho}{q_\varrho}$ nach der Grösse seines Abstandes von x in die Reihe der Näherungsbrüche einordnet.

Da vermöge der Gleichung

$$p_\varrho^2 - Dq_\varrho^2 = 1,$$

$$p_\varrho - q_\varrho\sqrt{D} = \frac{1}{p_\varrho + q_\varrho\sqrt{D}},$$

$$\frac{p_\varrho}{q_\varrho} - \sqrt{D} = \frac{1}{q_\varrho(p_\varrho + q_\varrho\sqrt{D})} = \frac{d}{q_\varrho^2},$$

also

$$d = \frac{q_\varrho}{p_\varrho + q_\varrho\sqrt{D}},$$

ist somit in unserem Falle zu zeigen, dass

$$\frac{q_\varrho}{p_\varrho + q_\varrho\sqrt{D}} < \frac{q_\varrho}{q_\varrho + q_{\varrho-1}}$$

oder

$$q_\varrho + q_{\varrho-1} < p_\varrho + q_\varrho\sqrt{D}.$$

Da

$$\frac{p_\varrho}{q_\varrho} > 1, \quad \sqrt{D} > 1, \quad q_{\varrho-1} \leqq q_\varrho,$$

wird in der That

$$q_\varrho < p_\varrho,$$

$$q_{\varrho-1} < q_\varrho\sqrt{D},$$

also

$$q_\varrho + q_{\varrho-1} < p_\varrho + q_\varrho\sqrt{D}.$$

Die Bedingung ist also erfüllt und es findet sich somit jeder durch eine Lösung p_ϱ, q_ϱ der Gleichung $t^2 - Du^2 = 1$ bestimmte Bruch $\frac{p_\varrho}{q_\varrho}$ unter den Näherungsbrüchen der Kettenbruchentwicklung für $\sqrt{D}$.

2. Da Zähler und Nenner der Näherungsbrüche beständig wachsen, so folgt, dass die Auflösung, welche man zuerst erhält, die kleinste ist. Nun erhält man aber am Schlusse der ersten, resp. zweiten Periode des Kettenbruches für $\sqrt{D}$ zum ersten Male eine Lösung, bei welcher u nicht 0, also muss diese abgesehen von den verschiedenen Vorzeichen, welche man ihr beilegen kann, die kleinste sein.

§ 2. Gauss.

Gauss löst die Gleichung $t^2 - Du^2 = 1$ als Spezialfall der allgemeineren Gleichung $t^2 - Du^2 = m^2$, indem er sich auf den Satz stützt (Disqu. Arith. Art. 162), dass aus zwei verschiedenen Transformationen einer Form

$$F = (A, B, C)$$

in eine andere Form $f = (a, b, c)$; $b^2 - ac = D$, eine von der Lösung $U = o$, $T = \pm m$ verschiedene Lösung T, U der Gleichung $T^2 - DU^2 = m^2$ folgt, wenn wir unter m den grössten gemeinschaftlichen Teiler der Zahlen a, $2b$, c verstehen.

Nachdem dann durch die Untersuchung des Äquivalenzproblems quadratischer Formen mit positiver nicht quadratischer Determinante Mittel gewonnen sind, eine Substitution einer Form der bezeichneten Art in sich selbst zu finden, liefert dieselbe im Verein mit der stets anwendbaren Substitution $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ eine positive Lösung der Gleichung $t^2 - Du^2 = 1$.

Da man es ferner so einrichten kann, dass die so erhaltene Lösung die kleinste ist, welche es giebt, so folgen aus ihr nach den schon von Lagrange bewiesenen Formeln alle übrigen.

Es würde somit zunächst der Satz aus Art. 162 der Disquisitionen zu beweisen sein. Da der Beweis jedoch bei Gauss mit sehr umständlichen Rechnungen verknüpft ist, und man für den vorliegenden Fall mit einer Spezialisierung jenes allgemeineren Gaussschen Theorems auskommt, beschränke ich mich darauf, dieselbe im Anschluss an Dirichlet zu beweisen.

Satz. Ist $\begin{pmatrix} \alpha_n & \beta_n \\ \gamma_n & \delta_n \end{pmatrix}$ eine Substitution, durch welche die Form (a, b, c) mit der positiven nicht quadratischen Determinante $D = b^2 - ac$ und dem Teiler m in sich selbst übergeführt wird, und setzt man

$$t = \pm \frac{m(\alpha_n + \delta_n)}{2}, \quad u = \pm \frac{\gamma_n m}{a} = \pm \frac{\beta_n m}{c},$$

so ist

$$t^2 - Du^2 = m^2.$$

Beweis.[1]) Da

$$(a, b, c); \begin{pmatrix} \alpha_n & \beta_n \\ \gamma_n & \delta_n \end{pmatrix}; (a, b, c),$$

so ist

$$\alpha_n \delta_n - \beta_n \gamma_n = 1,$$

$$a\alpha_n^2 + 2b\alpha_n\gamma_n + c\gamma_n^2 = a, \tag{1}$$

$$a\alpha_n\beta_n + (\alpha_n\delta_n + \beta_n\gamma_n)b + c\gamma_n\delta_n = b, \tag{2}$$

$$a\beta_n^2 + 2b\beta_n\delta_n + c\delta_n^2 = c. \tag{3}$$

Aus der zweiten Gleichung folgt, wenn man statt

$$\alpha_n\delta_n, \qquad \beta_n\gamma_n + 1$$

1) Dirichlet-Dedekind, Vorlesungen. IV. Aufl. S. 150 für komplexe Zahlen. Dirichlet: Sur les formes quadratiques à coefficients et à indéterminées complexes Crelle. Bd. 24. p. 291. Dirichlet, ges. Werke. Bd. I. Berlin 1880. S. 573.

setzt,

$$a\alpha_n\beta_n + 2b\beta_n\gamma_n + c\gamma_n\delta_n = 0$$

$$a\alpha_n^2 + 2b\alpha_n\gamma_n + c\gamma_n^2 = a,$$

$$-c(\alpha_n\gamma_n\delta_n - \gamma_n^2\beta_n) = a\beta_n.$$

$$o = a\beta_n + c\gamma_n \tag{4}$$

und

$$a(\alpha_n^2\delta_n - \alpha_n\beta_n\gamma_n) + 2b(\alpha_n\gamma_n\delta_n - \beta_n\gamma_n^2) = a\delta_n,$$

$$a\alpha_n + 2b\gamma_n = a\delta_n.$$

$$a(\alpha_n - \delta_n) + 2b\gamma_n = 0. \tag{5}$$

Da a nicht o, so folgt, wenn m der grösste gemeinsame Teiler von a, $2b$, c, und u eine beliebige ganze Zahl, aus (4)

$$\gamma_n = \frac{a}{m}u; \qquad \beta_n = \frac{-c}{m}u,$$

aus (5)

$$\alpha_n - \delta_n = \frac{-2b}{m}u.$$

Da nun

$$\alpha_n\delta_n - \beta_n\gamma_n = 1,$$

so giebt das

$$\alpha_n\delta_n = \beta_n\gamma_n + 1 = -\frac{ac}{m^2}u^2 + 1$$

und da

$$\alpha_n - \delta_n = \frac{-2b}{m}u,$$

$$(\alpha_n + \delta_n)^2 = \frac{4b^2u^2}{m^2} - \frac{4acu^2 - 4m^2}{m^2} = \frac{4\{Du^2 + m^2\}}{m^2}$$

oder

$$\left\{\frac{m(\alpha_n + \delta_n)}{2}\right\}^2 = Du^2 + m^2.$$

Die rechte Seite der Gleichung zeigt, dass $\frac{\pm m(\alpha_n + \delta_n)}{2}$ eine ganze Zahl; setzen wir sie gleich t, so kommt

$$t^2 = Du^2 + m^2$$

oder

$$t^2 - Du^2 = m^2,$$

wo

$$t = \pm \frac{m(\alpha_n + \delta_n)}{2}, \qquad u = \pm \frac{m\gamma_n}{a} = \mp \frac{m\beta_n}{c}$$

wie behauptet.

Da wir die Form (a, b, c) bis auf die Determinante und Teiler willkürlich wählen können, so leuchtet ein, dass jede Substitution irgend einer die zwei gleichen Invarianten besitzenden Form in sich selbst eine Lösung der Gleichung giebt.

Satz. Durch alle Substitutionen der Form (a, b, c) in sich selbst bekommt man alle Auflösungen der Gleichung $t^2 - Du^2 = m^2$.

Beweis. Wir führen den Beweis, indem wir zeigen, dass jeder Lösung t, u der Gleichung $t^2 - Du^2 = 1$ eine Substitution der Form (a, b, c) in sich selbst entspricht. Dann müssen umgekehrt alle Substitutionen alle Lösungen liefern.

Durch Auflösung der Definitionsgleichungen für t und u ergiebt sich

$$\alpha_n = \frac{t - bu}{m}, \qquad \beta_n = \frac{-cu}{m},$$

$$\gamma_n = \frac{au}{m}, \qquad \delta_n = \frac{t + bu}{m},$$

zugleich ist

$$t^2 - Du^2 = m^2.$$

Es muss zunächst gezeigt werden, dass m in die verschiedenen Zähler aufgeht. Dies ist von vornherein der Fall bei γ_n und β_n. Ferner ist

$$4t^2 - 4Du^2 = 4m^2;$$

in

$$4D = 4b^2 - 4ac$$

geht m^2 auf, auch wenn (a, b, c) keine primitive Form ist; also ist auch $\frac{4t^2}{m^2}$ eine ganze Zahl; ebenso $\frac{2t}{m}$ und daher $2\alpha_n$ und $2\delta_n$. Die Summe dieser beiden, nämlich $\frac{4t}{m}$, ist gerade, da $\frac{2t}{m}$ ganz, also sind $2\alpha_n$ und $2\delta_n$ entweder beide gerade oder beide ungerade. Nun ist aber ihr Produkt

$$4\alpha_n\delta_n = 4\frac{t^2 - b^2u^2}{m^2} = 4\left(1 - \frac{ac}{m^2}u^2\right)$$

gerade; somit gilt das gleiche von $2\alpha_n$ und $2\delta_n$, α_n und δ_n sind also ganze Zahlen. Führt man die Substitution

$$\alpha_n = \frac{t - bu}{m} \qquad \beta_n = -\frac{cu}{m},$$

$$\gamma_n = \frac{au}{m} \qquad \delta_n = \frac{t + bu}{m}$$

nunmehr aus, so kommt

$$a\left(\frac{t-bu}{m}\right)^2 + 2b \cdot \frac{-bau^2 + atu}{m^2} + c\,\frac{a^2u^2}{m^2} =$$
$$a\left\{\frac{t^2}{m^2} - \frac{2tbu}{m^2} + \frac{2tbu}{m^2} + \frac{acu^2}{m^2} - \frac{b^2u^2}{m^2}\right\} =$$
$$a\left\{\frac{t^2 - Du^2}{m^2}\right\} = a$$

und ebenso

$$a\,\frac{(t-bu)(-cu)}{m^2} + b\,\frac{(t^2 - bu^2) - acu^2}{m^2} + c\,\frac{(t+bu)\,au}{m^2} = b,$$

daher auch $c' = c$. Die Substitution führt also in der That (a, b, c) in sich selbst über.

Die Aufgabe, die Gleichung

$$t^2 - Du^2 = 1$$

zu lösen, ist also hierdurch auf die andere zurückgeführt, alle Substitutionen oder zum mindesten eine von der Substitution $\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$ verschiedene Substitution $\begin{pmatrix}\alpha_n & \beta_n\\ \gamma_n & \delta_n\end{pmatrix}$ aufzusuchen, welche eine eigentlich primitive Form der Determinante D in sich selbst transformieren.

Wir wollen daher von nun ab annehmen, der bisher m genannte Teiler sei gleich der Einheit, was offenbar erlaubt ist, da man zum mindesten in der stets vorhandenen, hier durch $(1, 0, -D)$ repräsentierten Hauptklasse lauter primitive Formen zur Verfügung hat.

Konstruktion (D. A. Art. 198).

Wir wählen eine reduzierte Form aus der Ordnung der eigentlich primitiven Klassen der Determinante D. Es sei die Form $(a, b, -a')$; sie sei ferner so gewählt, dass a positiv. Dann entwickeln wir die zu $(a, b, -a')$ gehörige Periode $(n = 2\nu)$,

$$(a, b, -a') = f,$$
$$(-a', b', a'') = f' \quad \text{etc. bis}$$
$$(a^{(n)}, b^{(n)}, -a^{(n+1)}) = f^{(n)} = f,$$

wo $f^{(n)}$ den Beginn der neuen, zweiten Periode bezeichnet. Bezeichnen wir ferner die Substitution, welche $f^{(k)}$ in seinen rechten Nachbar $f^{(k+1)}$ transformiert, mit

$$\begin{pmatrix} o & -1 \\ 1 & h^{(k+1)} \end{pmatrix} = S^{(k+1)},$$

so dass

$$f\left\{S^{(1)}\right\} f^{(1)} \left\{S^{(2)}\right\} f^{(2)} \ldots\ldots f^{(n-1)}\left\{S^{(n)}\right\} f^{(n)} = f,$$

dann führt die Substitution

$$\left\{S^{(1)}\right\} \left\{S^{(2)}\right\} \ldots\ldots \left\{S^{(n)}\right\} = \begin{pmatrix} \alpha_n & \beta_n \\ \gamma_n & \delta_n \end{pmatrix}$$

f in $f^{(n)}$, das heisst in sich selbst über.

Wir setzen nun

$$T = \pm \frac{\alpha_n + \delta_n}{2} \qquad U = \pm \frac{\gamma_{(n)}}{a}$$

und behaupten, dass

$$T^2 - DU^2 = 1,$$

dass U nicht o und dass T, U die kleinste (abgesehen vom Vorzeichen) Lösung der Gleichung $t^2 - Du^2 = 1$ ist, welche es giebt.

Beweis I. T, U sind ganzzahlig (incl. der o) und lösen die Gleichung

$$t^2 - Du^2 = 1;$$

denn da $\begin{pmatrix} \alpha_n & \beta_n \\ \gamma_n & \delta_n \end{pmatrix}$ f in sich selbst überführt, sind nach dem vorigen Satze T sowohl wie U ganzzahlig und genügen der Gleichung

$$t^2 - Du^2 = 1,$$

weil wir $m = 1$ gewählt haben.

II. U ist nicht o.

Bezeichnen wir den vierten Koeffizienten der Substitution $S^{(k)}$ inklusive seines Vorzeichens mit $h^{(k)}$, so hat $S^{(k)}$ die Form

$$\begin{pmatrix} o & -1 \\ 1 & h^{(k)} \end{pmatrix}.$$

Ist ferner die aus den ersten μ Substitutionen $S_1 \ldots S_u$ zusammengesetzte Substitution mit

$$\begin{pmatrix} \alpha_\mu & \beta_\mu \\ \gamma_\mu & \delta_\mu \end{pmatrix}$$

charakterisiert, so ist gemäss der Definition

$$\begin{pmatrix}\alpha_k & \beta_k\\ \gamma_k & \delta_k\end{pmatrix} = \begin{pmatrix}\alpha_{k-1} & \beta_{k-1}\\ \gamma_{k-1} & \delta_{k-1}\end{pmatrix}\begin{pmatrix}o & -1\\ +1 & h^{(k)}\end{pmatrix} = \begin{pmatrix}\beta_{k-1}; & \beta_{k-1}h^{(k)}-\alpha_{k-1}\\ \delta_{k-1}; & \delta_{k-1}h^{(k)}-\gamma_{k-1}\end{pmatrix},$$

also

$$\begin{pmatrix}\alpha_k = \beta_{k-1}; & \beta_k = \beta_{k-1}h^{(k)}-\alpha_{k-1}\\ \gamma_k = \delta_{k-1}; & \delta_k = \delta_{k-1}h^{(k)}-\gamma_{k-1}\end{pmatrix},$$

das giebt,

$\alpha_1 = o$	$\beta_1 = -1$	$\gamma_1 = 1$	$\delta_1 = h(^1)$
$\alpha_2 = \beta_1$	$\beta_2 = \beta_1\ h(^2) - \alpha_1$	$\gamma_2 = \delta_1$	$\delta_2 = \delta_1\ h(^2) - \gamma_1$
$\alpha_3 = \beta_2$	$\beta_3 = \beta_2\ h(^3) - \alpha_2$	$\gamma_3 = \delta_2$	$\delta_3 = \delta_2\ h(^3) - \gamma_2$ etc.

oder auch

$\alpha_1 = o$	$\beta_1 = -1$	$\gamma_1 = 1$	$\delta_1 = h(^1)$
$\alpha_2 = \beta_1$	$\beta_2 = h(^2)\ \beta_1$	$\gamma_2 = \delta_1$	$\delta_2 = h(^2)\ \delta_1 - 1$
$\alpha_3 = \beta_2$	$\beta_3 = h(^3)\ \beta_2 - \beta_1$	$\gamma_3 = \delta_2$	$\delta_3 = h(^3)\ \delta_2 - \delta_1$
$\alpha_4 = \beta_3$	$\beta_4 = h(^4)\ \beta_3 - \beta_2$	$\gamma_4 = \delta_3$	$\delta_4 = h(^4)\ \delta_3 - \delta_2$ etc.

Da wir ferner von der Form $(a, b, -a')$ ausgegangen sind, und da alle b positiv, wird

$$b + b' = -a'h(^1)$$
$$b' + b'' = a''h(^2)$$
$$b'' + b''' = -a'''h(^3) \text{ etc.}$$

$h^{(k)}$ hat also stets das gleiche Zeichen wie $a^{(k)}$. Wir wollen die absoluten Beträge der Grössen h mit den Buchstaben $k^{(1)}\ k^{(2)} \ldots . k^{(n)}$ bezeichnen. Dann ist (| · | bedeutet „absoluter Betrag" von)

$$(-1)\,\beta_1 = 1$$
$$(-1)\,\beta_2 = h^{(2)}\,(-\beta_1) = k^{(2)} \cdot 1 = k^{(2)}\ |\beta_1|$$
$$\beta_3 = (-k^{(3)})\,(-k^{(2)}) + 1 = k^{(3)}k^{(2)} + 1 = k^{(3)}|\beta_2| + |\beta_1|$$
$$\beta_4 = k^{(4)}\ |\beta_3| + k^{(2)} = k^{(4)}\ |\beta_3| + |\beta_2| \text{ etc.},$$
$$|\beta_k| = k^{(k)}\ |\beta_{k-1}| + |\beta_{k-2}|$$

und ebenso

$$|\delta_1| = -\delta_1 = |h^1| = k^{(1)}$$
$$|\delta_2| = -\delta_2 = h^{(2)}\,(-\delta_1) + 1 = k^{(2)}\ |\delta_1| + 1$$
$$|\delta_3| = \delta_3 = (-k^{(3)})\,\delta_2 - \delta_1 = k^{(3)}\ |\delta_2| + |\delta_1| \text{ etc.},$$
$$|\delta^k| = k^{(k)}\ |\delta_{k-1}| + |\delta_{k-2}|.$$

Die absoluten Beträge von δ_k und β_k werden also mit Hilfe von k_1 k_2 etc. nach demselben Gesetz gebildet, wie Zähler und Nenner der Näherungsbrüche des Kettenbruches

$$k_1 + \cfrac{1}{k_2 + \cfrac{1}{k_3 + \cfrac{1}{k_4 \text{ etc.},}}}$$

so dass wir für $|\delta_k|$ den Zähler des $k$ten Näherungsbruches, für $|\beta_k|$ den Nenner des nämlichen setzen dürfen. Hieraus geht aber hervor, dass $|\alpha_k|$ $|\delta_k|$ $|\beta_k|$ $|\gamma_k|$ mit dem Index k beständig wachsen, somit $\pm u = \frac{|\gamma_n|}{a}$ sicherlich von o verschieden ist.

Das Vorzeichen von α_n und γ_n bestimmt sich nach der Regel, dass es positiv, wenn $n \equiv o$ oder 1 (mod. 4), negativ, wenn $n \equiv 2$ oder 3 (mod. 4); δ_n und β_n sind positiv, wenn $n \equiv o$ oder $\equiv 3$ (mod. 4), negativ, wenn $n \equiv 1$ oder 2 (mod. 4).

$\frac{\gamma_n}{\alpha_n}$ und $\frac{\delta_n}{\beta_n}$ sind also stets positiv und daher gleich dem $n-1$ten und $n$ten Näherungsbruche von

$$k_1 + \cfrac{1}{k_2 + \cfrac{1}{k_3 \text{ etc.}}}$$

III. Die auf die angegebene Art erhaltene Lösung der Gleichung $t^2 - Du^2 = 1$ ist, abgesehen vom Vorzeichen, die kleinste.

Wir haben im Vorstehenden die Existenz beliebig vieler Lösungen nachweisen und Mittel geben können, sie aufzusuchen, ohne mehr als das Reduktionsverfahren und die Existenz von Perioden reduzierter Formen vorauszusetzen. Den Hauptsatz der Theorie, dass zwei äquivalente reduzierte Formen stets der gleichen Periode angehören, haben wir nicht zu benutzen nötig gehabt.

Für den gegenwärtigen Zweck sind jedoch die Prinzipien unentbehrlich, auf welche sich der Beweis jenes Hauptsatzes stützt, und es wird erforderlich auf den Zusammenhang der Substitutionen S und $\begin{pmatrix}\alpha & \beta \\ \gamma & \delta\end{pmatrix}$ mit den Wurzeln der reduzierten Formen einzugehen, sei es, dass man mit Dirichlet die Kettenbruchentwicklung derselben ausdrücklich in den Vordergrund stellt, sei es, dass man, wie Gauss, ich möchte sagen absichtlich, es vermeidet, diese Seite der Sache hervortreten zu lassen.

Um jedoch nicht die ganzen Fundamente der Theorie darlegen zu müssen, will ich voraussetzen, der Beweis des Hauptsatzes (D A. Art. 193) sei in der Gaussschen Weise erbracht. Dann ist gezeigt worden, dass jede Substitution $\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$, welche eine reduzierte Form f in eine andere F überführt, sich unter den Substitutionen befindet, welche durch Zusammensetzung beliebig vieler aufeinander folgender, von f aus nach rechts oder links führender Substitutionen $S^{(k)}$ oder $S^{(-k)}$ entstehen. Haben die Grössen $\frac{\alpha}{\gamma}$ und $\frac{\beta}{\delta}$ das gleiche Zeichen wie a, so befindet sich $\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$ unter den Substitutionen $\prod_1^k S^{(k)}$, haben sie das Zeichen von a', so ist $\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$ unter den Substitutionen $\prod_1^k S^{(-k)}$.

Nehmen wir nun an, es gebe eine Lösung T' U' der Gleichung $t^2 - Du^2 = 1$, so dass (T' und U' immer positiv genommen ebenso wie T und U), $U' < U$ also $T' < T$, wo T, U die auf die angegebene Weise aus der Substitution $\begin{pmatrix}\alpha_n & \beta_n\\ \gamma_n & \delta_n\end{pmatrix}$ gewonnene Lösung bezeichnen möge. Alsdann ist nach dem zweiten in diesem § bewiesenen Satze

$$\begin{pmatrix}\alpha' = T' - bU'; & \beta' = U'a'\\ \gamma' = U'a; & \delta' = T' + bU'\end{pmatrix}$$

eine Substitution der Form $(a, b, -a')$ in sich selbst.

Da wir T, U, T', U' als positiv voraussetzen und auch $a > o$ gewählt haben, so folgt

$$o < \gamma' < Ua = \gamma_n$$
$$o < \beta' < Ua' = \beta_n$$

und da

$$T^{(\prime)2} = DU^{(\prime)2} + 1 = b^2U^{(\prime)2} + aa'U^{(\prime)2} + 1$$
$$T^{(\prime)2} > b^2U^{(\prime)2}$$
$$T^{(\prime)} > bU^{(\prime)},$$

also

$$\alpha' = T^{(\prime)} - bU^{(\prime)} > o$$
$$\delta' > o.$$

$\begin{pmatrix}\alpha' & \beta'\\ \gamma' & \delta'\end{pmatrix}$ ist also eine aus positiven Koeffizienten bestehende Substitution von $(a, b, -a')$ in sich selbst; sie muss sich also unter den Substitutionen $\begin{pmatrix}\alpha_k & \beta_k\\ \gamma_k & \delta_k\end{pmatrix} = \prod_1^k S^{(k)}$ finden. Es sei etwa

$$\alpha' = \alpha_\mu \qquad \beta' = \beta_\mu$$
$$\gamma' = \gamma_\mu \qquad \delta' = \delta_\mu$$

Da nun alle Koeffizienten der Substitutionen $\begin{pmatrix} \alpha_k & \beta_k \\ \gamma_k & \delta_k \end{pmatrix}$ gleichzeitig wachsen, so dass

$$|\alpha_{k+1}| > |\alpha_k|; \quad |\beta_{k+1}| > |\beta_k|; \quad |\gamma_{k+1}| > |\gamma_k|; \quad |\delta_{k+1}| > |\delta_k|,$$

und da $\gamma' < \gamma_n$, so folgt, dass $\mu < n$ sein muss. Nun geht aber f vermöge $\begin{pmatrix} \alpha_\mu & \beta_\mu \\ \gamma_\mu & \delta_\mu \end{pmatrix}$ in f_μ über; es müsste also $f_\mu = f$ sein, entgegen der Voraussetzung, f_n sei die erste nach rechts gelegene Form, welche diese Eigenschaft besässe: μ kann also nicht kleiner sein als n. Dann ist es aber auch unmöglich, dass $\gamma' < \gamma_n$, also $U' < U$. U ist somit wie behauptet der kleinstmögliche Wert für u; T, U also die kleinste Lösung.

Vergleicht man die Art, wie Gauss die Gleichung $t^2 - Du^2 = 1$ auflöst, mit den früher besprochenen Methoden, so zeigt sich, dass die Prinzipien, welche Gauss benutzt, und der Zusammenhang, in welchem die Auflösung steht, neu sind und gänzlich von den bisher erwähnten abweichen. Durch den systematischen Aufbau, den die Arithmetik in den Disquisitionen findet, wird auch der Fermatschen Gleichung ihr Platz angewiesen und es werden ihre Beziehungen zu anderen Gebieten aufgedeckt, so dass es von diesem Augenblicke, strenggenommen, nicht mehr möglich ist, die Geschichte der speziellen Aufgabe losgelöst von der der Disziplin zu verfolgen. Der Algorithmus jedoch, welcher die eigentliche Lösung liefert, ist im Grunde mit dem von Euler und Lagrange identisch, wie das noch deutlicher hervortritt, wenn man die Theorie der binären quadratischen Formen mit positiver Determinante in der Dirichletschen Fassung in Vergleich zieht.

Gauss betont diesen Zusammenhang auch selbst, indem er sagt (Art. 202): „Omnes hae solutiones, si essentiam spectas, conveniunt cum ea, quam obtinemus, si in art. 198 formam reductam eam adoptamus in qua $a = 1$". In der That ist es bei dem Gaussschen Verfahren gleichgültig, welche reduzierte Form man zum Ausgangspunkte wählt, während man, wenn man von $(1, o, -D)$ ausgeht, durch die Substitution

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & \lambda \end{pmatrix} = \begin{pmatrix} -1 & -\lambda \\ 0 & -1 \end{pmatrix},$$

wo λ die grösste ganze Zahl in $\sqrt{D}$, zu der reduzierten Form

$$(1, \lambda, \lambda^2 - D)$$

gelangt.

§ 3. Dirichlet und Jakobi.

Unabhängig von einander haben Dirichlet und Jakobi 1837 die Bemerkung gemacht, dass die Fermatsche Gleichung mit Hilfe der Kreisteilungstheorie als möglich bewiesen und aufgelöst werden[1][2][3] kann.

Dirichlet hat dann in einem besonderen Aufsatze die Untersuchung für den Fall vollständig durchgeführt, dass D eine ungerade Primzahl ist.[4]

Ich werde mich im folgenden an die ursprüngliche Darstellung von Dirichlet halten, da die einfachere Beweisführung bei Bachmann[5] den Nachteil hat, die numerischen Werte von t und u nicht unmittelbar zu geben.

Ich führe zunächst den Hilfssatz aus der Theorie der Gleichung $X = \frac{x^D - 1}{x - 1} = 0$ an, nebst einer Folgerung aus demselben, deren man zum Beweise und zur Entwicklung des in Rede stehenden Verfahrens bedarf.

I. $$4X = Y^2 - (-1)^{\frac{D-1}{2}} DZ^2$$ (D. A. Art. 357).

Die Betrachtung von Gauss (Art. 356) nimmt ihren Ausgang von der quadratischen Gleichung, welche (D als ungerade Primzahl voraus-

1) Der ebenso einfache wie allgemeine Beweis, welchen Dirichlet in der Abhandlung, Sur les formes quadratiques à coefficients et à indéterminées complexes. § 13. Crelle. Bd. 24. p. 291 u. f. (1842). Ges. Werke. Bd. I. Berlin 1889. S. 578—582 gegeben hat, ist hier nicht mit reproduziert, da er nicht die Mittel zur wirklichen Lösung giebt. In gleicher Weise ist die Lösung der Gleichung $t^2 - Du^2 = 1$ nach der Dirichletschen vereinfachten Theorie der quadratischen Formen (Werke, Bd. II. Berlin 1897. S. 156 oder 177) mit positiver Determinante deswegen übergangen, weil die eigentliche Lösung sich von der Gaussschen der Sache nach nicht unterscheidet.

2) Dirichlet macht die Bemerkung zum ersten Mal in der Abhandlung. „Beweis des Satzes, dass jede arithmetische Progression deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Faktor sind, unendlich viel Primzahlen enthält.“ Abh. der königl. Akademie der Wissenschaften zu Berlin von 1837. S. 45 u. f. (Juli 1837 gel.) Ges. Werke. Bd. I. Berlin 1889; am Schlusse des § 4 l. c. S. 328.

3) Jakobi, Über die Kreisteilung und ihre Anwendung auf die Zahlentheorie.“ Auszug aus einem Schreiben an die Akad. der Wissensch. zu Berlin vom 16. Okt. 1837. Monatsberichte d. A. d. W. z. B. 1837. S. 137 u. f. Crelle. Bd. 30. S. 166. Ges. Werke. Bd. VI. Berlin 1891. S. 263. (Aus Vorlesung früherer Jahre!)

4) Dirichlet, Sur la manière de résoudre l'équation $t^2 - Du^2 = 1$ au moyen des fonctions circulaires. Crelle Journal etc. Bd. 17. p. 286. Ges. Werke. Bd. I. Berlin 1889 S. 343 u. f.

5) P. Bachmann, Vorlesungen über die Theorie der Kreisteilung. Leipzig 1870. S. 296.

gesetzt) die beiden $\frac{D-1}{2} = m$ gliedrigen Perioden $(m, 1)$, (m, g) des Wurzelkomplexes Ω der Gleichung $X = \frac{x^D - 1}{x - 1} = 0$ zu Wurzeln hat.

Es gehören zu $(m, 1)$ die Wurzeln

$$[1]\ [g^2]\ [g^4] \text{ bis } [g^{D-3}] \left(\text{Anzahl } \frac{D-1}{2}\right),$$

zu (m, g)

$$[g]\ [g^3]\ [g^5] \ldots . [g^{D-1}].$$

Bezeichnen wir die kleinsten Reste $(mod\ D)$ der Grössen

$$1\ g^2 \ldots g^{D-3}$$

mit

$$1\ R\ R_1 \ldots . R_{\left(\frac{D-5}{2}\right)},$$

(ohne Rücksicht auf die Ordnung), die der Grössen

$$g, g^3 \ldots . \text{ mit } N, N_1 \ldots .,$$

so ist

$$(m, 1) = [1] + [R] + [R_1] + \ldots .$$

$$(m, g) = [N] + [N_1] + [N_2] + \ldots .$$

Die Zahlen 1, R, R_1 sind nun sämtlich kleiner als D, in der Anzahl $\frac{D-1}{2}$ vorhanden und quadratische Reste zu D; da sie alle verschieden sind, müssen somit sämtliche quadratischen Reste kleiner als D sein, die es zu D giebt, und somit die Zahlen $N, N_1 \ldots .$ sämtlich Nichtreste.

Zugleich leuchtet gemäss der Definition von $[g^k]$ ein, dass alle Wurzeln in $\left(\frac{D-1}{2}, 1\right)$ resp. $(m, 1)$ Wurzeln der Gleichung

$$z = \left(x - e^{a_1 \frac{2\pi i}{D}}\right)\left(x - e^{a_2 \frac{2\pi i}{D}}\right) \ldots \ldots \left(x - e^{a_m \frac{2\pi i}{D}}\right) = 0,$$

alle Wurzeln der Periode $\left(\frac{D-1}{2}, g\right)$ Wurzeln der Gleichung

$$z_1 = \left(x - e^{b_1 \frac{2\pi i}{D}}\right)\left(x - e^{b_2 \frac{2\pi i}{D}}\right) \ldots \ldots \left(x - e^{b \frac{2\pi i}{D}}\right) = 0$$

sind, wenn wir statt $1_1 \ldots R_1$, R_2 etc. a_1, a_2 etc. statt N, N_1, N_2 etc. b, b_1 etc. setzen; ausserdem ist

$$zz_1 = \frac{x^D - 1}{x - 1} = X.$$

Berechnet man nun die Koeffizienten der quadratischen Gleichung, welche $(m, 1)$ und (m, g) zu Wurzeln hat, also die Aggregate $(m, 1) + (m, g)$ und $(m, 1) \times (m, g)$ nach den Vorschriften von Disqu. Arith. Art. 345 und 350, so ergiebt sich, wenn $\frac{D-1}{2}$ ungerade, also D von der Form $4k + 3$

$$x^2 + x + \frac{1}{4}(D + 1) = 0,$$

wenn $\frac{D-1}{2}$ gerade, also $D = 4k + 1$

$$x^2 + x - \frac{1}{4}(D - 1) = 0,$$

als die gesuchte Gleichung. Beide Fälle können wir zusammenfassen in der Form

$$x^2 + x + \frac{1 - (-1)^{\frac{D-1}{2}} D}{4} = 0.$$

Hieraus folgt

$$(m, 1) = -\frac{1 \pm \sqrt{(-1)^{\frac{D-1}{2}} D}}{2},$$

$$(m, g) = -\frac{1 \mp \sqrt{(-1)^{\frac{D-1}{2}} D}}{2}.$$

Nach dem Lehrsatze aus Art. 348 der Disqu. Arith. [Koeffizientenbestimmung der die Wurzeln einer Periode zu Wurzeln besitzenden Gleichung, mit Hilfe des Umstandes, dass die Koeffizienten symmetrische Funktionen der Perioden-Wurzeln] hat nun z die Form

$$z = R + S(m, 1) + T(m, g),$$

wo R, S und T ganze Funktionen von x mit ganzzahligen Koeffizienten bezeichnen. Von diesen Polynomen ist R vom $\frac{D-1}{2}$ ten, die übrigen von geringerem Grade.

Durch cyklische Vertauschung erhält man sodann

$$z' = R + S(m, g) + T(m, 1).$$

Setzt man $(m, 1) = p$, $(m, g) = q$, so kann man $2z$, resp. $2z_1$ schreiben, wie folgt:

$$2z = 2R + (T + S)(p + q) - (T - S)(p - q),$$
$$2z_1 = 2R + (T + S)(p + q) + (T - S)(p - q),$$

und da $p + q = -1$

$$2z_1 = 2R - T - S + (T - S)(p - q),$$
$$2z = 2R - T - S - (T - S)(p - q).$$

Oder wenn wir

$$2R - T - S = Y$$
$$T - S = Z$$

nennen,

(1)
$$2z = Y \pm Z\sqrt{(-1)^{\frac{D-1}{2}} D},$$
$$2z_1 = Y \mp Z\sqrt{(-1)^{\frac{D-1}{2}} D}$$

und hieraus durch Multiplikation

$$4zz_1 = 4X = Y^2 - (-1)^{\frac{D-1}{2}} DZ^2.$$

Der Satz gilt indes nur für den Fall, dass D eine Primzahl. Dirichlet giebt am Schlusse der Abhandlung „Sur la manière de résoudre etc." ohne Beweis seine Ausdehnung auf einen aus zwei Primzahlen p, q zusammengesetzten Wert $D = pq$. Dedekind hat das Theorem endlich auf den Fall ausgedehnt, wo D das Produkt aus beliebig vielen Primzahlen, jedoch ohne quadratischen Teiler[1]) ist.

II.
$$x^{\frac{D-1}{2}} Y\left(\frac{1}{x}\right) = Y(x); \quad x^{\frac{D-1}{2}} Z\left(\frac{1}{x}\right) = Z(x),$$

wenn

$$D = 4k + 1,$$

1) Dirichlet-Dedekind, Vorlesungen über Zahlentheorie. IV. Aufl. Braunschweig 1894. § 139 u. 140. p. 365 u. f., ferner § 107. p. 277 u. f. An dieser Stelle ist die Anwendung gemacht, sie liefert jedoch keine explizite Lösung. Ich gehe darum hier nicht darauf ein.

$$x^{\frac{D-1}{2}} Y\left(\frac{1}{x}\right) = - Y(x); \quad x^{\frac{D-1}{2}} Z\left(\frac{1}{x}\right) = Z(x),$$

wenn

$$D = 4k + 3.$$ [1]

Nach den Formeln S. 111 können wir die Ausdrücke für z und z_1 offenbar auch so schreiben

$$z(x) = \prod_\alpha (x - r^\alpha), \quad z_1(x) = \prod_\beta (x - r^\beta),$$

indem wir α das vollständige System quadratischer Reste zu D, welche kleiner als D, β die Nichtreste kleiner als D durchlaufen lassen.

Dann ist

$$(-x)^{\frac{D-1}{2}} z\left(\frac{1}{x}\right) = \prod_\alpha (x - r^{-\alpha}),$$

$$(-x)^{\frac{D-1}{2}} z_1\left(\frac{1}{x}\right) = \prod_\beta (x - r^{-\beta}).$$

Ist nun $D = 4k + 1$, so stimmen die Reste der Zahlen $-\alpha$ (mod. D) überein mit den Zahlen α selbst, die Reste der Zahlen $-\beta$ (mod. D) mit den Zahlen β, da die unter den Grössen $-\alpha$ befindliche negative Einheit quadratischer Rest zu allen Primzahlen von der Form $4k + 1$ ist, und die Grössen $-\alpha$ durch Multiplikation von (-1) und α, also durch Multiplikation zweier Reste entstehen.

Ist $D = 4n + 3$, so ist (-1) quadratischer Nichtrest zu D, die Zahlen $-\alpha$ bilden also ein vollständiges Nichtrestsystem und die Zahlen $-\beta$ ein vollständiges Restsystem.

Im ersten Falle hat man also

$$\prod_\alpha (x - r^{-\alpha}) = \prod_\alpha (x - r^{-\alpha}),$$

$$\prod_\beta (x - r^{-\beta}) = \prod_\beta (x - r^{-\beta})$$

oder

$$(-x)^{\frac{D-1}{2}} z\left(\frac{1}{x}\right) = z(x),$$

$$(-x)^{\frac{D-1}{2}} z_1\left(\frac{1}{x}\right) = z_1(x).$$

1) P. Bachmann, Vorlesungen über die Theorie der Kreisteilung. Leipzig 1870. S. 206.

Setzt man hier den für z resp. z_1 gefundenen Wert in die Gleichung (1) Seite 113 ein, so kommt

$$(-x)^{\frac{D-1}{2}}\left(Y\left(\tfrac{1}{x}\right) \pm Z\left(\tfrac{1}{x}\right)\sqrt{(-1)^{\frac{D-1}{2}}D}\right) = Y(x) \pm Z(x)\sqrt{(-1)^{\frac{D-1}{2}}D},$$

also

$$(-x)^{\frac{D-1}{2}}Y\left(\tfrac{1}{x}\right) = Y(x),$$

$$(-x)^{\frac{D-1}{2}}Z\left(\tfrac{1}{x}\right) = Z(x)$$

und da $\frac{D-1}{2}$ gerade

$$(x)^{\frac{D-1}{2}}Y\left(\tfrac{1}{x}\right) = Y(x),$$

$$(x)^{\frac{D-1}{2}}Z\left(\tfrac{1}{x}\right) = Z(x).$$

Im zweiten Falle, wo $D = 4k + 3$, wird in entsprechender Weise

$$-(x)^{\frac{D-1}{2}}z\left(\tfrac{1}{x}\right) = z_1(x);\quad -(x)^{\frac{D-1}{2}}z_1\left(\tfrac{1}{x}\right) = z(x),$$

$$-(x)^{\frac{D-1}{2}}\left(Y\left(\tfrac{1}{x}\right) \pm Z\left(\tfrac{1}{x}\right)\sqrt{(-1)^{\frac{D-1}{2}}D}\right) = Y(z) \mp Z(x)\sqrt{(-1)^{\frac{D-1}{2}}D},$$

also

$$x^{\frac{D-1}{2}}Y\left(\tfrac{1}{x}\right) = -\,Y(x),$$

$$x^{\frac{D-1}{2}}Z\left(\tfrac{1}{x}\right) = Z(x),\ q.\ e.\ d.$$

III. Lösung der Gleichung $t^2 - Du^2 = 1$.
Wir fanden (S. 111), dass $2z$ die Form hat

$$2z = Y(x) + Z(x)\sqrt{(-1)^{\frac{D-1}{2}}D}$$
$$= 2\left(x - e^{a_1\frac{2\pi i}{D}}\right)\left(x - e^{a_2\frac{2\pi i}{D}}\right)\ldots\ldots\left(x - e^{a_m\frac{2\pi i}{D}}\right),$$

oder da die Zahlen $a_1 \ldots a_{\left(\frac{D-1}{2}\right)}$ die Reste (*mod.* D) der Zahlen

$$1^2, 2^2 \ldots \tfrac{1}{4}(D-1)^2,$$

$$Y(x) + Z(x)\sqrt{(-1)^{\frac{D-1}{2}} D} = 2\left(x - e^{1^2 \frac{2\pi i}{D}}\right)\left(x - e^{2^2 \frac{2\pi i}{D}}\right) \text{ etc.}$$

(1.) Wir nehmen nun zunächst an, D habe die Form $4k + 1$ Alsdann wird die Gausssche Gleichung (Satz I dieses Paragraphen)

$$4X = Y^2 - DZ^2;$$

setzt man hierin die Variable $x = 1$, so wird

$$X = x^{D-1} + x^{D-2} + \ldots\ldots + x + 1 = D$$

und die ganzzahligen Funktionen $Y(x)$ und $Z(x)$ gleich g resp. h, so dass

$$4D = g^2 - Dh^2.$$

Hier kann weder g noch h Null sein, da D positiv und kein Quadrat Ferner muss g durch D teilbar sein. Setzen wir $g = Dk$, so kommt

$$4D = D^2k^2 - Dh^2$$

oder

$$h^2 - Dk^2 = -4.$$

Um aus der Lösung dieser Gleichung eine Lösung der Gleichung

$$t^2 - Du^2 = 1$$

abzuleiten, unterscheiden wir, je nachdem $D = 8\mu + 1$ oder $8\mu + 5$. Im ersten Fall müssen h und k beide gerade sein; denn zunächst können sie, da rechts -4 steht und $D = 8\mu + 1$ nur zugleich gerade oder ungerade sein; wären sie aber beide ungerade, so würde $h^2 \equiv 1 \pmod{8}$, $k^2 \equiv 1 \pmod{8}$, $k^2D \equiv 1 \pmod{8}$, $h^2 - k^2D \equiv o \pmod{8}$ sein, was nicht der Fall ist. Man darf also setzen

$$\left(\frac{h}{2}\right)^2 - D\left(\frac{k}{2}\right)^2 = -1,$$

und daher

$$\left\{\frac{1}{4}(h^2 + Dk^2)\right\}^2 - D\left\{\frac{2}{4}\,h\,k\right\}^2 = 1.$$

Ist zweitens $D = 8\mu + 5$, so können h und k gerade oder ungerade sein.[1]) Sind h und k gerade, so erhält man offenbar die gleiche Lösung

1) Dirichlet sagt irrtümlicher Weise, h und k müssten stets ungerade sein. Das ist jedoch schon für $D = 37$ nicht der Fall, wo man $h = 12$, $k = 2$ setzen

wie im vorigen Fall; sind sie ungerade, so setzen wir

$$(h + k\sqrt{D})^3 (h - k\sqrt{D})^3 = (-4)^3$$
$$= (h' + k'\sqrt{D})(h' - k'\sqrt{D}),$$

also

$$(h + k\sqrt{D})^3 = h' + k'\sqrt{D},$$

und daher

$$h' = h^3 - 3hk^2D,$$
$$k' = 3h^2k + k^3D.$$

Da nun

$$h^2 - Dk^2 = -4,$$

also

$$h^3 = Dhk^2 - 4h.$$

wird

$$h' = 4h(k^2D - 1)$$

und da

$$k^3D = h^2k + 4k,$$
$$k' = 4k(h^2 + 1).$$

Nun sind die beiden Ausdrücke in den Klammern gerade, also

$$h' \equiv o \pmod{8}, \quad k' \equiv o \pmod{8}.$$

Man darf also setzen, da

$$h'^2 - Dk'^2 = (-4)^3 = -8^2,$$
$$\left(\frac{h'}{8}\right)^2 - D\left(\frac{k'}{8}\right)^2 = -1$$

und somit

$$\left\{\frac{h'^2 + Dk'^2}{8}\right\}^2 - \left\{\frac{2h'k'}{8}\right\}^2 D = 1.$$

Man kann nun den Wert der Grössen h und k mit Hilfe von Kreisfunktionen vollständig angeben, ohne die Funktionen $Y(x)$ und $Z(x)$ erst berechnen zu müssen. Denn es ist

---

kann. Dedekind hat (Dirichlet, ges. Werke. Bd. II. Berlin 1897. p. 418) auf diesen Umstand aufmerksam gemacht und aus der Gleichung der Klassenanzahl n_D den Satz abgeleitet, dass h und k stets und nur dann gerade sind, wenn die Klassenanzahl durch 3 teilbar ist (vergl. auch D. A. Art. 256. VI).

$$2z(1) = g \pm h\sqrt{D}$$
$$= 2\left(1 - e^{1^2\frac{2\pi i}{D}}\right)\left(1 - e^{2^2\frac{2\pi i}{D}}\right)\dots\dots\left(1 - e^{m^2\frac{2\pi i}{D}}\right),$$

und da

$$1 - e^{s^2\frac{2\pi i}{D}} = 1 - e^{s^2\frac{\pi i}{D}}\, e^{s^2\frac{\pi i}{D}}$$
$$= 1 - \left\{\cos\left(s^2\frac{\pi}{D}\right) + i\sin\left(s^2\frac{\pi}{D}\right)\right\} e^{s^2\frac{\pi i}{D}}$$
$$= 1 - \left\{\cos\left(s^2\frac{\pi}{D}\right) + i\sin\left(s^2\frac{\pi}{D}\right)\right\}\cos\left(s^2\frac{\pi}{D}\right) - i\sin\left(s^2\frac{\pi}{D}\right) e^{s^2\frac{\pi i}{D}}$$
$$= -i\sin\left(s^2\frac{\pi}{D}\right) e^{s^2\frac{\pi i}{D}} - i\sin\left(s^2\frac{\pi}{D}\right) e^{s^2\frac{\pi i}{D}}$$
$$= -2i\sin\left(s^2\frac{\pi}{D}\right) e^{s^2\frac{\pi i}{D}}$$

wird, ist also

$$2z(1) = g \pm h\sqrt{D}$$
$$= 2^{\frac{D+1}{2}}(-i)^{\frac{D-1}{2}}\sin\left(1^2\frac{\pi}{D}\right)\sin\left(2^2\frac{\pi}{D}\right)\dots\dots\sin\left(\left[\frac{1}{2}(D-1)\right]^2\frac{\pi}{D}\right)$$
$$\times e^{\left\{1^2 + 2^2 + \dots + \left[\frac{1}{2}(D-1)\right]^2\right\}\frac{\pi i}{D}}.$$

Da nun $\frac{D-1}{2}$ gerade, wird

$$(-i)^{\frac{D-1}{2}} = (-1)^{\frac{D-1}{4}}.$$

Ferner ist

$$1^2 + 2^2 + 3^2 \text{ etc.} = D\,\frac{D^2-1}{24}.$$

Ist nun $D = 8\mu + 1$, so ist der Faktor $\frac{D-1}{2}$, der in $\frac{D^2-1}{24}$ steckt, gerade, also $\frac{D^2-1}{24}$ gerade. Ist $D = 8\mu + 5$, so ist

$$\frac{D^2-1}{24} = \frac{D-1}{4}\cdot\frac{D+1}{2}\cdot\frac{1}{3},$$

also sicher ungerade, da $\frac{D-1}{4}$ sowohl wie $\frac{D+1}{2}$ ungerade sind. Somit wird

$$e^{\left\{1^2 + 2^2 + \dots + \left[\frac{1}{2}(D-1)\right]^2\right\}\frac{\pi i}{D}} = e^{\frac{D-1}{24}\pi i},$$

also gleich $+1$, wenn $D = 8\mu + 1$ gleich -1, wenn $D = 8\mu + 5$. Beide Fälle kann man zusammenfassen, indem man schreibt

$$e^{[1^2 + 2^2 + \ldots] \frac{\pi i}{D}} = (-1)^{\frac{D-1}{4}}.$$

Dann wird

$$g + h\sqrt{D} = 2^{\frac{D-1}{2}} \sin\left(1^2 \frac{\pi}{D}\right) \sin\left(2^2 \frac{\pi}{D}\right) \ldots\ldots$$
$$\ldots \sin\left\{\left(\frac{D-1}{2}\right)^2 \frac{\pi}{D}\right\}$$

und

$$h + k\sqrt{D} = \frac{2^{\frac{D-1}{2}}}{\sqrt{D}} \sin\left(1^2 \frac{\pi}{D}\right) \ldots\ldots \sin\left\{\left(\frac{D-1}{2}\right)^2 \frac{\pi}{D}\right\} = \alpha,$$

ferner da

$$h^2 - k^2 D = -4,$$

$$h \mp k\sqrt{D} = \frac{-4}{\alpha}$$

und somit

$$h = \pm\left(\frac{\alpha}{2} - \frac{2}{\alpha}\right); \quad k = \pm \frac{1}{\sqrt{D}}\left(\frac{\alpha}{2} + \frac{2}{\alpha}\right).$$

Es sind also h und k vollkommen bestimmt.

(2). D habe die Form $4k + 3$.

Dann ist nach dem zweiten Satze dieses Paragraphen

$$(x)^{\frac{D-1}{2}} Y\left(\frac{1}{x}\right) = -Y(x),$$

$$(x)^{\frac{D-1}{2}} Z\left(\frac{1}{x}\right) = Z(x).$$

Giebt man hierin x den Wert i, so kommt

$$-i^{\frac{D-1}{2}} Y(-i) = Y(i)$$

und

$$i^{\frac{D-1}{2}} Z(-i) = Z(i).$$

Da Y und Z nun ganze Funktionen sind, wird

$$Y(i) = g + g'i$$

und

$$Z(i) = h + h'i,$$

wo h, h', g, g' ganze reelle Zahlen.

Wir unterscheiden wieder zwei Fälle, je nachdem $D = 8\mu + 3$ oder $D = 8\mu + 7$.

Im ersten Falle wird

$$i^{\frac{D-1}{2}} = i,$$

also

$$Y(i) = g + g'i = -i(g - g'i),$$
$$Z(i) = h + h'i = i(h - h'i)$$

und da hieraus folgt, dass

$$g = -g', \quad h = h',$$

so ist

$$Y(i) = g(1 - i), \quad Z(i) = h(1 + i).$$

Im zweiten Falle, wo $D = 8\mu + 7$, wird

$$i^{\frac{D-1}{2}} = -i,$$

somit

$$Y(i) = g + g'i = i(g - g'i),$$
$$Z(i) = h + h'i = -i(h - h'i),$$

also

$$g = g', \quad h = -h'$$

und daher

$$Y(i) = g(1 + i), \quad Z(i) = h(1 - i).$$

Durch die Substitution $x = i$ erhält man ferner

$$X(i) = \frac{i^D - 1}{i - 1}$$

und dies wird, da $D = 4k + 3$

$$\frac{-i - 1}{i - 1} = i.$$

Die Gleichung

$$4X = Y^2 + DZ^2$$

liefert also für den Fall, dass $D = 4k + 3$, die folgende

$$4X(i) = Y(i)^2 + DZ(i)^2,$$

also

$$4i = g^2 (1 \mp i)^2 + Dh^2 (1 \pm i)^2.$$

Nun ist aber

$$(1 \pm i)^2 = \pm 2i,$$

daher

$$\pm 2 = g^2 - Dh^2,$$

und endlich

$$\left(\frac{g^2 + h^2 D}{2}\right)^2 - D (gh)^2 = 1,$$

wobei der erste Wert jedenfalls ganz ist, da g und h vermöge der Gleichung $\pm 2 = g^2 - Dh^2$ nur gleichzeitig gerade und ungerade sein können; überdies ist nur der letztere Fall möglich, da sonst die rechte Seite der Gleichung $\pm 2 = g^2 - Dh^2$ durch 4 teilbar wäre, die linke aber nicht.

Es bleiben somit nur noch auch für diesen Fall die Grössen g und h zu berechnen.[1])

Nun ist aber[2])

$$\begin{aligned} Y(i) + i\sqrt{D}\, Z(i) &= g (1 \mp i) + i \sqrt{D}\, h (1 \pm i) \\ &= (1 \mp i) \left\{g \mp \sqrt{D}\, h\right\} \\ &= 2 \left(i - e^{1^2 \frac{2\pi i}{D}}\right) \left(i - e^{2^2 \frac{2\pi i}{D}}\right) \ldots \left(i - e^{\left(\frac{D-1}{2}\right)^2 \frac{2\pi i}{D}}\right). \end{aligned}$$

Bezeichnen wir mit s eine der Zahlen von 1 bis $\frac{D-1}{2}$ und schreiben wir statt $s^2 \frac{2\pi i}{D}$ zur Abkürzung $2\lambda i$, so ist

$$\begin{aligned} (i - e^{2\lambda i}) &= i \left\{1 + i e^{2\lambda i}\right\} = i \left\{1 + e^{\left(2\lambda + \frac{\pi}{2}\right) i}\right\} \\ &= i \left\{1 + e^{2\left(\lambda + \frac{\pi}{4}\right) i}\right\} = i \left\{1 + e^{2\lambda' i}\right\} \\ &= i \left\{1 + (\cos \lambda' + i \sin \lambda')\, e^{\lambda' i}\right\} \\ &= i \left\{1 + \cos \lambda'\, e^{\lambda' i} + i \sin \lambda' (\cos \lambda' + i \sin \lambda')\right\} \end{aligned}$$

---

1) Dirichlet deutet diese Rechnung nur an.

2) Vergl. Seite 113 unten.

$$= 2i \cos \lambda' e^{\lambda' i} = 2i\, e^{\frac{\pi}{4} i} \cos \lambda' e^{\lambda i}$$

$$= 2i \left(\cos \frac{\pi}{4} + i \sin \frac{\pi}{4} \right) \cos \lambda' e^{\lambda i}$$

$$= 2i \left(\sqrt{\frac{1}{2}} + i \sqrt{\frac{1}{2}} \right) \cos \lambda' e^{\lambda i}$$

$$= \sqrt{2}\,(i - 1) \cos \lambda' e^{\lambda i}.$$

Somit wird

$$(i \mp 1)(g \mp h\sqrt{D})$$

$$(\sqrt{2})^{\frac{D+3}{2}} (i-1)^{\frac{D-1}{2}} \cos\left\{1^2 \frac{\pi}{D} + \frac{\pi}{4}\right\} \cos\left\{2^2 \frac{\pi}{D} + \frac{\pi}{4}\right\} \cdots$$

$$\cdots \cos\left\{\left(\frac{D-1}{2}\right)^2 \frac{\pi}{D} + \frac{\pi}{4}\right\} e^{\left[1^2 + 2^2 + \cdots + \left(\frac{D-1}{2}\right)^2\right] \frac{\pi i}{D}}$$

rechts und links hebt sich einmal (ob. Zeichen) $(i - 1)$, es bleibt rechts $(i-1)^{\frac{D-3}{2}}$. D hat die Form $8\mu + 3$ oder $8\mu + 7$. Also wird im ersten Falle, da

$$(+)^2 (i-1)^2 = -2i,$$

$$(i-1)^{\frac{D-3}{2}} = 2^{\frac{D-3}{4}} \cdot (-1)^{\frac{D-3}{8}}.$$

Ist dagegen D von der Form $8\mu + 7$, so gilt das untere Zeichen und man hat

$$(i-1)^{\frac{D-1}{2}} = (i-1)^{4\mu+3} = -(2i)^{2\mu}(2i)(i-1)$$

$$= 2 \cdot (2i)^{2\mu} (i+1) = 2^{2\mu+1} (-1)^{\mu} (i+1)$$

$$= 2^{\frac{D-3}{4}} (-1)^{\frac{D-7}{8}} (i+1).$$

Es hebt sich also $i + 1$ fort.

Der letzte Faktor wird in beiden Fällen

$$e^{\frac{D^2-1}{24} \pi i}, \quad \text{wo} \quad \frac{D^2-1}{24}$$

vermöge seiner Entstehungsweise notwendig ganzzahlig ist.

Ist nun $D = 8\mu + 3$, so ist

$$\frac{D^2-1}{24} = \frac{(D+1)}{4} \cdot \frac{(D-1)}{2} \frac{1}{3}$$
$$= \frac{8\mu+4}{4} \cdot \frac{8\mu+2}{2} \cdot \frac{1}{3}$$

jedenfalls ungerade,

$$e^{\frac{D^2-1}{24}\pi i} \text{ also } = -1.$$

Ist $D = 8\mu + 7$, so wird

$$\frac{D^2-1}{24} = \frac{(D+1)}{8} \cdot \frac{(D-1)}{3} = \frac{(8\mu+8)}{8} \cdot \frac{(8\mu+6)}{3}$$

jedenfalls gerade und somit

$$e^{\frac{D^2-1}{24}\pi i} = 1.$$

Beide Fälle lassen sich zusammenfassen in die Formel:

$$e^{\frac{D^2-1}{24}\pi i} = (-1)^{\frac{1}{4}(D+1)}.$$

Es wird daher (das obere Zeichen für $D = 8\mu + 3$)

$$g + h\sqrt{D}$$
$$= (-1)^{\frac{3D \mp 1 \atop \mp 5}{8}} (\sqrt{2})^D \cos\left\{1^2 \frac{\pi}{D} + \frac{\pi}{4}\right\} \ldots\ldots \cos\left\{\left(\frac{D-1}{2}\right)^2 \frac{\pi}{D} + \frac{\pi}{4}\right\}$$
$$= \alpha.$$

Nun war

$$g^2 - Dh^2 = \pm 2,$$

also ist

$$g - h\sqrt{D} = \pm \frac{2}{\alpha}$$

und folglich

$$g = \frac{\alpha}{2} \pm \frac{1}{\alpha}; \quad h = \frac{1}{\sqrt{D}} \left\{\frac{\alpha}{2} \mp \frac{1}{\alpha}\right\}.$$

Damit ist auch für den Fall

$$D = 4k + 3,$$

die Gleichung $t^2 - Du^2 = 1$ vollständig gelöst.

Es bleibt noch zu bemerken, dass die mit Hilfe des Gaussschen Satzes gefundenen Lösungen der Fermatschen Gleichung keineswegs die kleinsten sind, wie man sie nach den früher besprochenen Methoden erhält. Ihr Zusammenhang mit den letztgenannten Zahlen ist durch die Dirichletschen Untersuchungen über die Klassenanzahl der quadratischen Formen aufgedeckt worden; doch muss ich mich damit begnügen, die Gleichung anzugeben, durch welche die kleinste Lösung und die aus der Theorie der Kreisteilung sich ergebende mit einander verknüpft sind. Ist D eine positive Primzahl von der Form $4k+1$, H die Klassenanzahl, T, U die kleinste Lösung der Gleichung $t^2 - Du^2 = 1$, während h, k die gleiche Bedeutung haben wie bisher, so wird

$$(T + U\sqrt{D})^H = \left(\frac{h + k\sqrt{D}}{2}\right)^{4 - 2\left(\frac{2}{D}\right)}$$

und allgemein für jede Primzahl D

$$(T + U\sqrt{D})^H = \left(\frac{Y(1) + Z(1)\sqrt{D}}{2\sqrt{D}}\right)^{4 - 2\left(\frac{2}{D}\right)}.$$

§ 4. Seit Dirichlet.

Wir haben bei früherer Gelegenheit bemerkt, dass Wallis sowohl wie Euler der Meinung waren, man dürfe bei der Kettenbruchentwicklung von $\sqrt{D}$ zum Zweck der Auflösung der Fermatschen Gleichung nach Belieben positive und negative Teilnenner benutzen, dass jedoch Lagrange in seinen Additions zu Eulers Algebra an einem Beispiel zeigte, dass dies keineswegs erlaubt ist, und man Gefahr läuft, niemals zum Ziele zu gelangen.

Wann dies letztere jedoch eventuell eintrete, hatte Lagrange nicht untersucht.

Diese Frage wurde nun von Stern[1]), Minnigerode[2]) und Roberts[3]) aufgegriffen, und es zeigte sich, dass es doch die Gleichung

1) Stern, Über die Eigenschaften der periodischen negativen Kettenbrüche, welche die Quadratwurzel aus einer ganzen positiven Zahl darstellen. Abhandl der königl. Ges. der Wiss. z. Göttingen. 1866. Bd. 12. S. 3—48.

2) B. Minnigerode, Über eine neue Methode, die Pellsche Gleichung aufzulösen. Nachrichten von der königl. Ges. der Wiss. z. Göttingen. Nr. 23. 20. Aug. 1873. Göttingische gelehrte Anzeigen 1873. Bd. III. S. 619.

3) S. Roberts, Note on the Pellian Equation. Proceedings of the London Math. Society. Vol. XV. Nov. 1883 bis Nov. 1884. p. 247. London.

$t^2 - Du^2 = 1$ mit Hilfe von Kettenbrüchen mit negativen Teilnennern zu lösen gelingt, sofern die Teilnenner nicht sämtlich negativ sind und gewissen Bedingungen genügen.

Sobald diese letzteren einmal festgestellt sind, ist der Weg zur Lösung vollkommen der gleiche, wie er sich aus der Gauss-Dirichletschen Theorie der quadratischen Formen mit positiver nicht quadratischer Determinante ergiebt, nur dass es notwendig wird, die reduzierten Formen in abweichender Weise zu definieren.

Es wird also mit Hilfe der Kettenbruchentwicklung einer Wurzel einer reduzierten Form, jedesmal eine Substitution gefunden, welche zu einer beliebigen anderen Form der Periode hinüberführt. Hat man zur zweiten Form eine solche gewählt, welche der ersten gleich ist, so erhält man eine Substitution der Form in sich selbst; es lässt sich zugleich fast genau wie bei der Benutzung gewöhnlicher Kettenbruchentwicklungen zeigen, dass man auf dem angegebenen Wege alle Substitutionen der gewählten reduzierten Form in sich selbst erhält.

Alsdann ergeben sich ebenso wie früher alle Lösungen der Gleichung

$$t^2 - Du^2 = m^2$$

(m der grösste gemeinschaftliche Teiler der 3 Koeffizienten $a, 2b, c$) aus allen gefundenen Substitutionen.

Ich beschränke mich daher mit Rücksicht auf die Analogie des Verfahrens darauf, einige Punkte hervorzuheben.

Es sei w eine positive oder negative irrationale Zahl, grösser als Zwei; a_0 die w am nächsten liegende ganze Zahl; dann setzen wir

$$w = a_0 - \frac{1}{w_1}, \quad a_0 \geqq 2;$$

nun ist

$$-\frac{1}{2} < \frac{1}{w_1} < \frac{1}{2},$$

somit

$$|w_1| > 2$$

und daher

$$w_1 = a_1 - \frac{1}{w_2} \text{ etc.}$$

$$w_{\nu-1} = a_{\nu-1} - \frac{1}{w_\nu}.$$

Da

$$|w_\nu| > 2,$$

so folgt aus der Gleichung

$$\frac{1}{w_\nu} + w_{\nu-1} = a_{\nu-1},$$

dass w_ν und $w_{\nu-1}$ verschiedene Vorzeichen haben, wenn $a_{\nu-1} = \pm 2$; da nun $a_{\nu-1}$ und $w_{\nu-1}$ das gleiche Zeichen haben, wird w_ν positiv oder negativ, je nachdem in der Gleichung

$$w_{\nu-1} = +2 - \frac{1}{w_\nu},$$

die 2 positiv oder negativ zu nehmen ist; w_ν hat dann das entgegengesetzte Zeichen. Also wird

$$w = a_0 - \cfrac{1}{a_1 - \cfrac{1}{a_2 - \cdots - \cfrac{1}{a_{\nu-1} - \cfrac{1}{w_\nu}}}},$$

wo stets $|a_k| \geq 2$, und wo a_{k+1} das entgegengesetzte Zeichen von a_k hat, wenn dieses gleich ± 2; die vollständigen Teilnenner w_k sind ihrem absoluten Betrage nach sämtlich grösser als 2. Es lässt sich zeigen, dass die letztgenannte Eigenschaft und die beiden erstgenannten sich gegenseitig bedingen.

Solche Kettenbrüche werden nun zur Lösung des Problems benutzt.

Es sei (a, b, c) eine Form mit positiver Determinante D und so beschaffen, dass der absolute Betrag der ersten Wurzel nämlich

$$\left|\frac{-b-\sqrt{D}}{c}\right| > 2; \quad |c| \geq |a|.$$

Derartige Formen werden für den gegenwärtigen Zweck „reduzierte" genannt. Es lässt sich zeigen, dass sie nur in endlicher Zahl vorhanden sein können.

Zunächst ist der alsolute Betrag der zweiten Wurzel kleiner als $\frac{1}{2}$, denn da

$$\frac{1}{2}(-b-\sqrt{D})(-b+\sqrt{D})\,2 = ac$$

und

$$\left|\frac{-b-\sqrt{D}}{c}\right| > 2,$$

folgt

$$\left|\frac{-b+\sqrt{D}}{a}\right| < \frac{1}{2},$$

also a fortiori

$$\left|\frac{-b+\sqrt{D}}{c}\right| < \frac{1}{2},$$

oder auch

$$\left|\frac{-b-\sqrt{D}}{2}\right| > 2,$$

es ist also gleichgültig, welche dieser vier letzten Bedingungen man wählt.

Endlich wird, wenn

$$b < \sqrt{D}, \ \frac{1}{2}(b+\sqrt{D}) > 2(-b+\sqrt{D}),$$

$$b > \sqrt{D}, \ \frac{1}{2}(b+\sqrt{D}) > 2(b-\sqrt{D}),$$

somit (b wird stets positiv)

$$\frac{3}{5}\sqrt{D} < b < \frac{5}{3}\sqrt{D}.$$

Es giebt also nur eine endliche Anzahl Werte für b, und da das gleiche für a und c aus der Gleichung $b^2 - D = ac$ folgt, so giebt es nur eine endliche Anzahl Formen, deren erste Wurzel absolut genommen > 2 und deren 3. Koeffizient abgesehen vom Zeichen grösser als der erste ist.

Doch brauchen durchaus nicht alle Formen, welche den Bedingungen

$$\frac{3}{5}\sqrt{D} < b < \frac{5}{3}\sqrt{D}$$

und $b^2 - D = ac$ genügen, die letztgenannten Eigenschaften zu besitzen.

Endlich ist zu bemerken, dass a und c entgegengesetzte Zeichen haben müssen, wenn $b < \sqrt{D}$, gleiche, wenn $b > \sqrt{D}$.

Wählt man nun eine beliebige Form (a, b, a') und entwickelt ihre erste Wurzel in einen Kettenbruch der oben bezeichneten Art (hier braucht $|a_0|$ nicht ≥ 2 zu sein), so entsprechen den vollständigen Teilnennern w_1 etc. benachbarte Formen, deren erste Wurzeln sämtlich absolut genommen grösser als 2 sind; setzt man ihre Kette genügend weit fort, so muss notwendig einmal der Fall eintreten, dass $|a_{(k+1)}| \geq |a_k|$,

da die absoluten Beträge der ganzen Zahlen $| a_k |$ nicht beliebig lange abnehmen können. An dieser Stelle hat man somit eine „reduzierte" Form. Setzt man die Reihe fort, so können die absoluten Beträge $| a_{k+2} |$ etc. wieder abnehmen; aber nicht gar lange; dann ist der an der Stelle $k + 1$ erhaltene Zuwachs erschöpft, und es tritt wiederum der Fall ein, dass der dritte Koeffizient der nächstbenachbarten Form abgesehen vom Vorzeichen grösser ist als der erste.

So fährt man fort und erhält beliebig viele „reduzierte Formen". Da es deren aber, wie gezeigt, nur eine beschränkte Anzahl giebt, so muss nach einer gewissen Zeit eine wiederkehren, die schon einmal da war. Von diesem Augenblicke ab wiederholt sich dann die ganze Formenkette, welche seit dem ersten Erscheinen von f passiert ist.

Es wird also die Formenkette, sowie die Kettenbruchentwicklung periodisch, und jede Periode enthält zum mindesten eine „reduzierte" Form.

Von diesem Punkte ab lässt sich die Untersuchung nun genau so weiter führen, wie bei der Benutzung gewöhnlicher Kettenbrüche, wie wir schon eingangs andeuteten. Es lässt sich auf die gleiche Weise zeigen, dass jede aus der Kettenbruchentwicklung der ersten Wurzel der reduzierten Form f gewonnene Substitution von f in sich selbst, eine Lösung der Gleichung

$$t^2 - Du^2 = m^2$$

liefert, dass man so alle diese Lösungen erhält, und dass jede reduzierte Form mit dem Teiler m mit gleichem Erfolge benutzt werden kann, sofern man nur berücksichtigt, dass die Eigenschaft in einen Kettenbruch der bezeichneten Art entwickelbar zu sein, für die reduzierten Formen charakteristisch ist.

In Anwendung auf die Fermatsche Gleichung ergiebt sich somit folgendes Verfahren: (1) Es muss sich stets eine „reduzierte" Form zum mindesten mit dem Teiler 1 finden lassen, da man von jeder eigentlich primitiven Form (a, b, c) z. B. $(1, o, D)$ zu einer solchen gelangen kann.

Giebt es mehrere, so wählt man eine aus und entwickelt ihre erste Wurzel in einen Kettenbruch der oben bestimmten Art; derselbe wird rein periodisch. Aus den Zählern und Nennern der zu den beiden letzten Plätzen der Periode gehörigen Näherungsbrüchen gewinnt man eine Substitution von (a, b, c) in sich selbst. Nennen wir die am Ende der ersten Periode erhaltene

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix},$$

so werden

$$u = \pm \frac{\beta}{c} = \mp \frac{\gamma}{a}$$

$$t = \pm \frac{\alpha + \delta}{2},$$

die kleinste Auflösung der Gleichung $t^2 - Du^2 = 1$ bilden.

Wir sind damit fast bei der unmittelbaren Gegenwart angelangt und verweisen den Leser für die weitere Verfolgung der Theorie unserer Gleichung auf die Schriften Kroneckers, in denen die Fermatsche Gleichung in ganz neuem Zusammenhange auftritt. Der Kreis, der durch die ältere Geschichte und Theorie geöffnet war, ist abgeschlossen, und so erübrigt es nur noch, der zahlreichen neueren Schriften zu gedenken, die sich mit der Gleichung $t^2 - Du^2 = 1$ befassen, ohne doch allgemeine Lösungsmethoden zu geben. Man findet in denselben eine Menge spezieller Fälle aufgelöst, Tabellen der kleinsten Lösungen berechnet[1]), ferner die Aufgabe behandelt, Wertreihen für D aufzustellen, bei welchen sich die kleinste Lösung unmittelbar geben lässt, kurz ein sehr reichliches Material, was die wirkliche Berechnung von Tabellen anlangt, die noch über den Umfang der Degenschen hinaus gehen sollen. (Man vergleiche die folgende Übersicht.)

Berkhan, Lehrbuch der unbestimmten Analytik. 2. Bd. Halle 1855—1856. Bd. II. p. 121.

Bells, Martin, Hart, Evans, Satz über die Auflage der Gleichungen $Ax^2 + 1 = Z^2$, $Ax^2 - 1 = Z^2$. Ed. Times XXIII. p. 96, 98, 109.

Cayley, Note sur l'équation $x^2 - Dy^2 = \pm 4$, $D \equiv 5 \pmod 8$. Crelle. Bd. 53. Berlin 1857. p. 369. Coll. Papers. Bd. IV. p. 40.

Canon Pellianus, sive tabula simplicissimam aequationis celebratissimae $y^2 = ax^2 + 1$ solutionem pro singulis numeri dati valoribus ab 1 usque ad 1000 in numeris rationalibus iisdemque integris exhibens. Autore Carolo Ferdinando Degen. Hafniae 1817, ebenso genaue Rechnung, wie gewähltes Latein; von Legendre bei der 3. Aufl. der „Theorie des nombres" benutzt.

Egen, Handbuch der allgemeinen Arithmetik. 2. Bd. Berlin 1846 u. 49. Bd. II. p. 468. Bd. I. p. 456.

Göpel, De aequationibus secundi gradus indeterminatis. Crelle. Bd. 45. p. 1. Berlin 1853.

Hart, H., New method of solving equations of the form of $x^2 - Ay^2 = 1$. Educ. Times XXVIII. p. 29.

1) Vor allem von Degen: canon Pellianus.

Hoffmann, Über Kettenbruchentwicklung und die Pellsche Gleichung. Grunerts Archiv (64). 1879. p. 1—8.

Hurwitz, Über eine besondere Art der Kettenbruchentwicklung reeller Grössen. Acta mathematica. Bd. 12. p. 367. Stockholm 1889.

Martin, A., Solution of a problem (Lösung von $x^2 - 9817\,y^2 = 1$). x hat 97, y 95 Stellen. Analyst. V. p. 118.

Meissel, E., Beitrag zur Pellschen Gleichung höherer Grade. Progr. der Ober-Realschule zu Kiel 1891.

Meyer, Über eine Eigenschaft der Pellschen Gleichung. Vierteljahrschrift der naturforschenden Gesellschaft in Zürich XXXII. p. 363. 1889.

Öttinger, Über das Pellsche Problem. Grunerts Archiv. Bd. 49. 1868. p. 193.

Pistor, Über die Auflösung der unbestimmten Gleichung 2. Grades in ganzen Zahlen; Programm, Hamm 1833.

Roberts, On Forms of Numbers determined by Continued Fractions. Proc. of the London math. soc. X. 1878. p. 29.

W. Schmidt, Über die Auflösung der Gleichung $t^2 - Du^2 = \pm 4$. Schlömilchs Zeitschrift XIX. p. 92, 1876.

Seeling, Über die Auflösung der Gleichung $x^2 - Ay^2 = \pm 1$ in ganzen Zahlen. Hoppe-Grunert Archiv LII. p. 40—49. 1870.

Smith, Note on the theorie of the Pellian equation. Proc. of the London Math. Society 1876. VII. p. 149. Coll. Papers Bd. II. p. 148.

Speckmann, Fundamentalauflösung der Pellschen Gleichung. Hoppe-Grunert Archiv (2). XIII. p. 216. 1894.

Speckmann, Über die Auflösung der Pellschen Gleichung. Hoppe-Grunert Archiv (2). XIII. p. 130. 1894.

Stern, Theorie der Kettenbrüche. Crelles Journal. Bd. 11. Berlin 1834. p. 331. § 116.

Stern, Zur Theorie der Periodischen Kettenbrüche. Crelle. Bd. 53. Berlin 1857. p. 1.

G. W. Tenner, Einige Bemerkungen über die Gleichung $ax^2 \pm 1 = y^2$. Programm Merseburg 1841. 4°.

Trattini, Dell equatione di Pell. Giornale matema'iche ed. Battaglini. Napoli XXX (3). p. 371. 1895.

Namen-Verzeichnis.

Druck von August Pries in Leipzig.





folgt

$$\left|\frac{-b+\sqrt{D}}{a}\right| < \frac{1}{2},$$

also a fortiori

$$\left|\frac{-b+\sqrt{D}}{c}\right| < \frac{1}{2},$$

oder auch

$$\left|\frac{-b-\sqrt{D}}{2}\right| > 2,$$

es ist also gleichgültig, welche dieser vier letzten Bedingungen man wählt.

Endlich wird, wenn

$$b < \sqrt{D}, \ \frac{1}{2}(b+\sqrt{D}) > 2(-b+\sqrt{D}),$$

$$b > \sqrt{D}, \ \frac{1}{2}(b+\sqrt{D}) > 2(b-\sqrt{D}),$$

somit (b wird stets positiv)

$$\frac{3}{5}\sqrt{D} < b < \frac{5}{3}\sqrt{D}.$$

Es giebt also nur eine endliche Anzahl Werte für b, und da das gleiche für a und c aus der Gleichung $b^2 - D = ac$ folgt, so giebt es nur eine endliche Anzahl Formen, deren erste Wurzel absolut genommen > 2 und deren 3. Koeffizient abgesehen vom Zeichen grösser als der erste ist.

Doch brauchen durchaus nicht alle Formen, welche den Bedingungen

$$\frac{3}{5}\sqrt{D} < b < \frac{5}{3}\sqrt{D}$$

und $b^2 - D = ac$ genügen, die letztgenannten Eigenschaften zu besitzen.

Endlich ist zu bemerken, dass a und c entgegengesetzte Zeichen haben müssen, wenn $b < \sqrt{D}$, gleiche, wenn $b > \sqrt{D}$.

Wählt man nun eine beliebige Form (a, b, a') und entwickelt ihre erste Wurzel in einen Kettenbruch der oben bezeichneten Art (hier braucht $|a_0|$ nicht ≥ 2 zu sein), so entsprechen den vollständigen Teilnennern w_1 etc. benachbarte Formen, deren erste Wurzeln sämtlich absolut genommen grösser als 2 sind; setzt man ihre Kette genügend weit fort, so muss notwendig einmal der Fall eintreten, dass $|a_{(k+1)}| \geq |a_k|$,

so folgt aus der Gleichung

$$\frac{1}{w_\nu} + w_{\nu-1} = a_{\nu-1},$$

dass w_ν und $w_{\nu-1}$ verschiedene Vorzeichen haben, wenn $a_{\nu-1} = \pm 2$; da nun $a_{\nu-1}$ und $w_{\nu-1}$ das gleiche Zeichen haben, wird w_ν positiv oder negativ, je nachdem in der Gleichung

$$w_{\nu-1} = +2 - \frac{1}{w_\nu},$$

die 2 positiv oder negativ zu nehmen ist; w_ν hat dann das entgegengesetzte Zeichen. Also wird

$$w = a_0 - \cfrac{1}{a_1 - \cfrac{1}{a_2 - \cdots - \cfrac{1}{a_{\nu-1} - \cfrac{1}{w_\nu}}}},$$

wo stets $|a_k| \geq 2$, und wo a_{k+1} das entgegengesetzte Zeichen von a_k hat, wenn dieses gleich ± 2; die vollständigen Teilnenner w_k sind ihrem absoluten Betrage nach sämtlich grösser als 2. Es lässt sich zeigen, dass die letztgenannte Eigenschaft und die beiden erstgenannten sich gegenseitig bedingen.

Solche Kettenbrüche werden nun zur Lösung des Problems benutzt.

Es sei (a, b, c) eine Form mit positiver Determinante D und so beschaffen, dass der absolute Betrag der ersten Wurzel nämlich

$$\left|\frac{-b-\sqrt{D}}{c}\right| > 2; \quad |c| \geq |a|.$$

Derartige Formen werden für den gegenwärtigen Zweck „reduzierte“ genannt. Es lässt sich zeigen, dass sie nur in endlicher Zahl vorhanden sein können.

Zunächst ist der alsolute Betrag der zweiten Wurzel kleiner als $\frac{1}{2}$, denn da

$$\frac{1}{2}(-b-\sqrt{D})(-b+\sqrt{D})\,2 = ac$$

und

$$\left|\frac{-b-\sqrt{D}}{c}\right| > 2,$$

folgt

$$\left|\frac{-b+\sqrt{D}}{a}\right| < \frac{1}{2},$$

also a fortiori

$$\left|\frac{-b+\sqrt{D}}{c}\right| < \frac{1}{2},$$

oder auch

$$\left|\frac{-b-\sqrt{D}}{2}\right| > 2,$$

es ist also gleichgültig, welche dieser vier letzten Bedingungen man wählt.

Endlich wird, wenn

$$b < \sqrt{D}, \quad \frac{1}{2}(b+\sqrt{D}) > 2(-b+\sqrt{D}),$$

$$b > \sqrt{D}, \quad \frac{1}{2}(b+\sqrt{D}) > 2(b-\sqrt{D}),$$

somit (b wird stets positiv)

$$\frac{3}{5}\sqrt{D} < b < \frac{5}{3}\sqrt{D}.$$

Es giebt also nur eine endliche Anzahl Werte für b, und da das gleiche für a und c aus der Gleichung $b^2 - D = ac$ folgt, so giebt es nur eine endliche Anzahl Formen, deren erste Wurzel absolut genommen > 2 und deren 3. Koeffizient abgesehen vom Zeichen grösser als der erste ist.

Doch brauchen durchaus nicht alle Formen, welche den Bedingungen

$$\frac{3}{5}\sqrt{D} < b < \frac{5}{3}\sqrt{D}$$

und $b^2 - D = ac$ genügen, die letztgenannten Eigenschaften zu besitzen.

Endlich ist zu bemerken, dass a und c entgegengesetzte Zeichen haben müssen, wenn $b < \sqrt{D}$, gleiche, wenn $b > \sqrt{D}$.

Wählt man nun eine beliebige Form (a, b, a') und entwickelt ihre erste Wurzel in einen Kettenbruch der oben bezeichneten Art (hier braucht $|a_0|$ nicht ≥ 2 zu sein), so entsprechen den vollständigen Teilnennern w_1 etc. benachbarte Formen, deren erste Wurzeln sämtlich absolut genommen grösser als 2 sind; setzt man ihre Kette genügend weit fort, so muss notwendig einmal der Fall eintreten, dass $|a_{(k+1)}| \geq |a_k|$,

so folgt aus der Gleichung

$$\frac{1}{w_\nu} + w_{\nu-1} = a_{\nu-1},$$

dass w_ν und $w_{\nu-1}$ verschiedene Vorzeichen haben, wenn $a_{\nu-1} = \pm 2$; da nun $a_{\nu-1}$ und $w_{\nu-1}$ das gleiche Zeichen haben, wird w_ν positiv oder negativ, je nachdem in der Gleichung

$$w_{\nu-1} = +2 - \frac{1}{w_\nu},$$

die 2 positiv oder negativ zu nehmen ist; w_ν hat dann das entgegengesetzte Zeichen. Also wird

$$w = a_0 - \cfrac{1}{a_1 - \cfrac{1}{a_2 - \cdots - \cfrac{1}{a_{\nu-1} - \cfrac{1}{w_\nu}}}},$$

wo stets $|a_k| \geq 2$, und wo a_{k+1} das entgegengesetzte Zeichen von a_k hat, wenn dieses gleich ± 2; die vollständigen Teilnenner w_k sind ihrem absoluten Betrage nach sämtlich grösser als 2. Es lässt sich zeigen, dass die letztgenannte Eigenschaft und die beiden erstgenannten sich gegenseitig bedingen.

Solche Kettenbrüche werden nun zur Lösung des Problems benutzt.

Es sei (a, b, c) eine Form mit positiver Determinante D und so beschaffen, dass der absolute Betrag der ersten Wurzel nämlich

$$\left|\frac{-b-\sqrt{D}}{c}\right| > 2; \quad |c| \geq |a|.$$

Derartige Formen werden für den gegenwärtigen Zweck „reduzierte“ genannt. Es lässt sich zeigen, dass sie nur in endlicher Zahl vorhanden sein können.

Zunächst ist der alsolute Betrag der zweiten Wurzel kleiner als $\frac{1}{2}$, denn da

$$\frac{1}{2}(-b-\sqrt{D})(-b+\sqrt{D})\,2 = ac$$

und

$$\left|\frac{-b-\sqrt{D}}{c}\right| > 2,$$

folgt

$$\left|\frac{-b+\sqrt{D}}{a}\right| < \frac{1}{2},$$

also a fortiori

$$\left|\frac{-b+\sqrt{D}}{c}\right| < \frac{1}{2},$$

oder auch

$$\left|\frac{-b-\sqrt{D}}{2}\right| > 2,$$

es ist also gleichgültig, welche dieser vier letzten Bedingungen man wählt.

Endlich wird, wenn

$$b < \sqrt{D}, \quad \frac{1}{2}(b+\sqrt{D}) > 2\,(-b+\sqrt{D}),$$

$$b > \sqrt{D}, \quad \frac{1}{2}(b+\sqrt{D}) > 2\,(b-\sqrt{D}),$$

somit (b wird stets positiv)

$$\frac{3}{5}\sqrt{D} < b < \frac{5}{3}\sqrt{D}.$$

Es giebt also nur eine endliche Anzahl Werte für b, und da das gleiche für a und c aus der Gleichung $b^2 - D = ac$ folgt, so giebt es nur eine endliche Anzahl Formen, deren erste Wurzel absolut genommen > 2 und deren 3. Koeffizient abgesehen vom Zeichen grösser als der erste ist.

Doch brauchen durchaus nicht alle Formen, welche den Bedingungen

$$\frac{3}{5}\sqrt{D} < b < \frac{5}{3}\sqrt{D}$$

und $b^2 - D = ac$ genügen, die letztgenannten Eigenschaften zu besitzen.

Endlich ist zu bemerken, dass a und c entgegengesetzte Zeichen haben müssen, wenn $b < \sqrt{D}$, gleiche, wenn $b > \sqrt{D}$.

Wählt man nun eine beliebige Form (a, b, a') und entwickelt ihre erste Wurzel in einen Kettenbruch der oben bezeichneten Art (hier braucht $|a_0|$ nicht ≥ 2 zu sein), so entsprechen den vollständigen Teilnennern w_1 etc. benachbarte Formen, deren erste Wurzeln sämtlich absolut genommen grösser als 2 sind; setzt man ihre Kette genügend weit fort, so muss notwendig einmal der Fall eintreten, dass $|a_{(k+1)}| \geq |a_k|$,

so folgt aus der Gleichung

$$\frac{1}{w_\nu} + w_{\nu-1} = a_{\nu-1},$$

dass w_ν und $w_{\nu-1}$ verschiedene Vorzeichen haben, wenn $a_{\nu-1} = \pm 2$; da nun $a_{\nu-1}$ und $w_{\nu-1}$ das gleiche Zeichen haben, wird w_ν positiv oder negativ, je nachdem in der Gleichung

$$w_{\nu-1} = \pm 2 - \frac{1}{w_\nu},$$

die 2 positiv oder negativ zu nehmen ist; w_ν hat dann das entgegengesetzte Zeichen. Also wird

$$w = a_0 - \cfrac{1}{a_1 - \cfrac{1}{a_2 - \cfrac{\cdot}{\cdot \; \cdot - \cfrac{1}{a_{\nu-1} - \cfrac{1}{w_\nu}}}}},$$

wo stets $|a_k| \geqq 2$, und wo a_{k+1} das entgegengesetzte Zeichen von a_k hat, wenn dieses gleich ± 2; die vollständigen Teilnenner w_k sind ihrem absoluten Betrage nach sämtlich grösser als 2. Es lässt sich zeigen, dass die letztgenannte Eigenschaft und die beiden erstgenannten sich gegenseitig bedingen.

Solche Kettenbrüche werden nun zur Lösung des Problems benutzt.

Es sei (a, b, c) eine Form mit positiver Determinante D und so beschaffen, dass der absolute Betrag der ersten Wurzel nämlich

$$\left|\frac{-b-\sqrt{D}}{c}\right| > 2; \quad |c| \geqq |a|.$$

Derartige Formen werden für den gegenwärtigen Zweck „reduzierte" genannt. Es lässt sich zeigen, dass sie nur in endlicher Zahl vorhanden sein können.

Zunächst ist der alsolute Betrag der zweiten Wurzel kleiner als $\frac{1}{2}$, denn da

$$\frac{1}{2}(-b-\sqrt{D})(-b+\sqrt{D})\,2 = ac$$

und

$$\left|\frac{-b-\sqrt{D}}{c}\right| > 2,$$

folgt

$$\left|\frac{-b+\sqrt{D}}{a}\right| < \frac{1}{2},$$

also a fortiori

$$\left|\frac{-b+\sqrt{D}}{c}\right| < \frac{1}{2},$$

oder auch

$$\left|\frac{-b-\sqrt{D}}{2}\right| > 2,$$

es ist also gleichgültig, welche dieser vier letzten Bedingungen man wählt.

Endlich wird, wenn

$$b < \sqrt{D}, \quad \frac{1}{2}(b+\sqrt{D}) > 2(-b+\sqrt{D}),$$

$$b > \sqrt{D}, \quad \frac{1}{2}(b+\sqrt{D}) > 2(b-\sqrt{D}),$$

somit (b wird stets positiv)

$$\frac{3}{5}\sqrt{D} < b < \frac{5}{3}\sqrt{D}.$$

Es giebt also nur eine endliche Anzahl Werte für b, und da das gleiche für a und c aus der Gleichung $b^2 - D = ac$ folgt, so giebt es nur eine endliche Anzahl Formen, deren erste Wurzel absolut genommen > 2 und deren 3. Koeffizient abgesehen vom Zeichen grösser als der erste ist.

Doch brauchen durchaus nicht alle Formen, welche den Bedingungen

$$\frac{3}{5}\sqrt{D} < b < \frac{5}{3}\sqrt{D}$$

und $b^2 - D = ac$ genügen, die letztgenannten Eigenschaften zu besitzen.

Endlich ist zu bemerken, dass a und c entgegengesetzte Zeichen haben müssen, wenn $b < \sqrt{D}$, gleiche, wenn $b > \sqrt{D}$.

Wählt man nun eine beliebige Form (a, b, a') und entwickelt ihre erste Wurzel in einen Kettenbruch der oben bezeichneten Art (hier braucht $|a_0|$ nicht $\geqq 2$ zu sein), so entsprechen den vollständigen Teilnennern w_1 etc. benachbarte Formen, deren erste Wurzeln sämtlich absolut genommen grösser als 2 sind; setzt man ihre Kette genügend weit fort, so muss notwendig einmal der Fall eintreten, dass $|a_{(k+1)}| \geqq |a_k|$,

so folgt aus der Gleichung

$$\frac{1}{w_\nu} + w_{\nu-1} = a_{\nu-1},$$

dass w_ν und $w_{\nu-1}$ verschiedene Vorzeichen haben, wenn $a_{\nu-1} = \pm 2$; da nun $a_{\nu-1}$ und $w_{\nu-1}$ das gleiche Zeichen haben, wird w_ν positiv oder negativ, je nachdem in der Gleichung

$$w_{\nu-1} = +2 - \frac{1}{w_\nu},$$

die 2 positiv oder negativ zu nehmen ist; w_ν hat dann das entgegengesetzte Zeichen. Also wird

$$w = a_0 - \cfrac{1}{a_1 - \cfrac{1}{a_2 - \cdots - \cfrac{1}{a_{\nu-1} - \cfrac{1}{w_\nu}}}},$$

wo stets $|a_k| \geqq 2$, und wo a_{k+1} das entgegengesetzte Zeichen von a_k hat, wenn dieses gleich ± 2; die vollständigen Teilnenner w_k sind ihrem absoluten Betrage nach sämtlich grösser als 2. Es lässt sich zeigen, dass die letztgenannte Eigenschaft und die beiden erstgenannten sich gegenseitig bedingen.

Solche Kettenbrüche werden nun zur Lösung des Problems benutzt.

Es sei (a, b, c) eine Form mit positiver Determinante D und so beschaffen, dass der absolute Betrag der ersten Wurzel nämlich

$$\left|\frac{-b-\sqrt{D}}{c}\right| > 2; \quad |c| \geqq |a|.$$

Derartige Formen werden für den gegenwärtigen Zweck „reduzierte" genannt. Es lässt sich zeigen, dass sie nur in endlicher Zahl vorhanden sein können.

Zunächst ist der alsolute Betrag der zweiten Wurzel kleiner als $\frac{1}{2}$, denn da

$$\frac{1}{2}(-b-\sqrt{D})(-b+\sqrt{D})\,2 = ac$$

und

$$\left|\frac{-b-\sqrt{D}}{c}\right| > 2,$$

folgt

$$\left|\frac{-b+\sqrt{D}}{a}\right| < \frac{1}{2},$$

also a fortiori

$$\left|\frac{-b+\sqrt{D}}{c}\right| < \frac{1}{2},$$

oder auch

$$\left|\frac{-b-\sqrt{D}}{2}\right| > 2,$$

es ist also gleichgültig, welche dieser vier letzten Bedingungen man wählt.

Endlich wird, wenn

$$b < \sqrt{D}, \quad \frac{1}{2}(b+\sqrt{D}) > 2(-b+\sqrt{D}),$$

$$b > \sqrt{D}, \quad \frac{1}{2}(b+\sqrt{D}) > 2(b-\sqrt{D}),$$

somit (b wird stets positiv)

$$\frac{3}{5}\sqrt{D} < b < \frac{5}{3}\sqrt{D}.$$

Es giebt also nur eine endliche Anzahl Werte für b, und da das gleiche für a und c aus der Gleichung $b^2 - D = ac$ folgt, so giebt es nur eine endliche Anzahl Formen, deren erste Wurzel absolut genommen > 2 und deren 3. Koeffizient abgesehen vom Zeichen grösser als der erste ist.

Doch brauchen durchaus nicht alle Formen, welche den Bedingungen

$$\frac{3}{5}\sqrt{D} < b < \frac{5}{3}\sqrt{D}$$

und $b^2 - D = ac$ genügen, die letztgenannten Eigenschaften zu besitzen.

Endlich ist zu bemerken, dass a und c entgegengesetzte Zeichen haben müssen, wenn $b < \sqrt{D}$, gleiche, wenn $b > \sqrt{D}$.

Wählt man nun eine beliebige Form (a, b, a') und entwickelt ihre erste Wurzel in einen Kettenbruch der oben bezeichneten Art (hier braucht $|a_0|$ nicht ≥ 2 zu sein), so entsprechen den vollständigen Teilnennern w_1 etc. benachbarte Formen, deren erste Wurzeln sämtlich absolut genommen grösser als 2 sind; setzt man ihre Kette genügend weit fort, so muss notwendig einmal der Fall eintreten, dass $|a_{(k+1)}| \geqq |a_k|$,